BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE HANDBOOK 31-223
1 FEBRUARY 1997

Security

THE AIR FORCE RESOURCE PROTECTION PROGRAM

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil. If you lack access, contact your Publishing Distribution Office (PDO).

This handbook is designed to help commanders and resource protection program managers better understand and apply Air Force and Department of Defense (DoD) resource protection criteria. It incorporates regulatory requirements while acknowledging the need for flexibility in light of unique mission requirements, threat levels, fiscal restraints, and other factors. This handbook covers protection criteria published in AFI 31-209, The Air Force Resource Protection Program; DoD 5100.76-M, Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives; Mil-Hdbk-1013/1, Military Handbook, Design Guidelines for Physical Security of Fixed Land-Based Facilities, and other references cited herein. Combined with those references, this handbook will help you meet both regulatory requirements and the spirit and intent of DoD and Air Force protection standards.

SUMMARY OF REVISIONS

This is the initial publication of Air Force Handbook 31-223.

OPR: HQ AFSPA/SPLE ((SMSgt Steven J. Peterson))

Certified by: HQ USAF/SP (Brig Gen R. A. Coleman)

Pages: 29/Distribution: F

Paragraph

Paragraph

Page

Chapter 1

RESPONSIBILITIES

1.1. Program Overview. The protection of Air Force resources is a great responsibility and one of our highest mission priorities. The sheer number and volume of Air Force resources make for challenging program management. Recent force restructuring and budget-cutting only enhance this challenge. This handbook is designed to help you evaluate from the top down, our resource protection measures and the programs that administer them. It supplies the information necessary to evaluate current protection guidance, modify existing measures, or develop new protection programs. It is not intended to act as a stand alone reference or information source. Instead, it summarizes and/or directs you to the many resource protection standards found in Air Force and Department of Defense (DoD) publications. Resource protection is a complex business, and consequently so are many of the references governing the protection of military assets. Where lengthy reproduction of protection criteria is not appropriate, we will refer to the governing directive. This manual, when combined with a sincere interest in resource protection, will insure full program compliance and a sound resource protection program.

1.2. Resource Protection Philosophy. The Air Force resource protection program is a challenging, dynamic program designed to protect a wide spectrum of resources. From the enlisted club to combat aircraft, your resource protection program must protect resources ranging from those seemingly less important, to those absolutely essential to our national security and war fighting capability. Yet there are no unimportant resources. Therefore, all personnel responsible for using, supporting, and protecting Air Force resources regardless of actual or perceived importance must thoroughly understand and implement your protection program. As you will see, everyone involved with the resource protection program plays a vital and specific role. Each must know their responsibilities if the program is to function as intended.

1.3. Installation Commander. The installation commander is the most important person in the resource protection program at your base. MAJCOMs, The Air Force Chief of Security Police, and various Air Staff agencies all have significant resource protection responsibilities, however, it's the installation commander who must implement policy and develop programs that will ensure the safety and security of war fighting assets. Chapters 1 and 2 of AFI 31-209, The Air Force Resource Protection Program, outlines the installation commander's responsibilities. The decisions made by the installation commander in the areas that follow are critical and will determine how resources are protected, and perhaps more importantly, the overall protection climate on the installation. For example, the installation commander:

1.3.1. Establishes the Resource Protection Executive Committee (RPEC). The RPEC is the primary vehicle for planning, managing and protecting resources. The RPEC advises the installation commander on many resource protection issues and is composed of senior installation commanders and advisors having broad levels of responsibility. Representation from key support agencies such as security police, staff judge advocate, and civil engineering is critical. The installation commander determines what agencies are represented on the RPEC.

Keep membership to a minimum but ensure adequate expertise and command representation. Members of the RPEC must remain familiar with their specific responsibilities contained in chapters 1 and 2 of AFI 31-209. Regardless of those

responsibilities, their only purpose is to help the installation commander protect installation resources through sound advise, research, planning, and enforcement of protection standards.

1.3.1.1. Determines the frequency and need for RPEC meetings. AFI 31-209 requires the RPEC to convene annually; however, more frequent meetings are encouraged, depending on type of resources assigned, threat analysis, current situation, and installation commander's judgment. Regardless of how often meetings are convened, it's important that the installation commander make known his or her concerns and program objectives well in advance of the meeting. The RPEC is a decision making body; consequently complete plans, policies, recommendations and other staffing details must be complete before the meeting convenes. Distribute agendas, proposals, and all necessary support material to RPEC members (and key subordinate working groups) well in advance. It's important that RPEC members familiarize themselves with each agenda item that will require their recommendation. The installation commander and key RPEC members should assign members of their staff to work closely with the installation Chief of Security Police (CSP) and the base Resource Protection Program Manager (RPPM) to research, coordinate, and pre-brief critical RPEC agenda items.

1.3.1.1.1. Record official minutes of the RPEC meeting and distribute meeting minutes according to local procedure. At a minimum, RPEC meeting minutes should include the following: 1) name, rank, and organization of key personnel in attendance; 2) date and time the meeting is convened and ended; 3) outline of each main issue briefed, name of the briefer and/or the issue OPR; 4) summary of floor discussion and recommendation; 5) all final decisions and directives that effect plans, policy, or procedure; 6) list of personnel or units tasked to perform research, supply information or accomplish tasks in support of the RPEC agenda; and 7) summary of decisions made and open items to address at the next RPEC meeting

1.3.2. Establishes RPEC Working Groups. Upon completion of a new, or review and approval of an existing installation resource protection plan, (IRPP) the installation commander determines the need for RPEC working groups. When established, these groups work under the direction and authority of the RPEC. There are four common working groups: Threat Working Group; Loss Prevention Working Group; Plans Working Group; and Alarm Working Group. The IRPP and content of the installation's initial review (conducted IAW program reviews requirement, chapter 2, AFI 31-209) will generally supply the installation commander with the information necessary to determine the need to establish additional working groups. These two documents are the critical tools an installation commander uses to assess the vulnerabilities and security needs of their installation. Consequently periodic review is essential to keep them current. This responsibility normally falls to the chairperson of the threat working group if such a group is formed. AFI 31-209 chapter 1, contains mandatory RPEC working group responsibilities, and initial review requirements are outlined in chapter 2.

1.4. Installation Chief of Security Police. With the exception of the installation commander, the CSP carries the greatest responsibility for installation security and resource protection. The CSP is the installation commander's primary advisor for the resource protection program and serves as the office of primary responsibility (OPR) for the wing's resource protection program. Unless otherwise directed by the installation commander, the CSP chairs the threat working group when this group is established. The CSP develops the documents discussed in para 1.3.2 of this manual, and performs additional duties outlined in AFI 31-209.

1.4.1. Resource Protection Program Manager: Each CSP appoints a RPPM to assist with the many resource protection responsibilities. Unit size, mission, threat, types of resources and other factors determine if this position is a full time responsibility or combined with another collateral functions, such as OIC/NCOIC of Information, Personnel, or Industrial Security. However, unless the above factors support otherwise, the nature and complexity of resource protection generally merits a full time position devoted to that function.

1.4.1.1. Qualifications. Select a capable officer or NCO with strong communications and staffing capabilities to fill this key position. Remember, the RPPM is a key orator and guide for RPEC working groups, and your manager for an installation wide program. When filling this position, consider each candidate's depth and degree of security, resource protection, and managerial experience. There is no minimum grade requirement for the RPPM position, however, it is wise to select a grade commensurate with the responsibilities outlined above and those contained in AFI 31-209.

1.4.1.2. Training. The base RPPM as well as other key resource protection staff members should attend formal resource protection training. Attend course WCIP07A -Resource Protection/Crime Prevention Theory, Practice, and Management - PDS Code 1F2, at Eastern Kentucky University. Funding for this course is determined by the MAJCOM RPPM or Installation Commander. Unit resource protection program managers and supervisors with significant resource protection responsibilities should enroll in ECI course 8100, the USAF Crime Prevention Program. Additionally, those personnel waiting to attend course WCIPO07A should also enroll unless they expect to attend the in-residence course within three months of their assignment of resource protection responsibilities.

1.4.1.3. Responsibilities. In addition to duties outlined in chapter 1, AFI 31-209, the RPPM oversees the training of unit resource protection focal points. It's important that each unit focal point for resource protection receive initial program orientation, and training. Document and file orientation and training. Scope and depth of training is a local matter determined by the needs of the unit. Things to consider are: size and geography of the unit and its resources; type, size, and value of its

assigned resources; history of pilferage, theft, damage, or loss; type and reliability of existing safeguards; contents of previous program reviews and the IRPP. Remember, training should vary with the needs of each particular wing and therefore tailored to meet individual unit needs. Unless similar units with like resource protection needs are trained together, mass training and "packaged" material (for the purpose of initial focal point training) are discouraged and do not meet the intent of the Air Force Resource Protection Program.

1.5. Unit Commanders. Close coordination with the RPPM and the CSP are two of your greatest responsibilities relating to the protection of resources. Conversely, both are required to assist you in reviewing your unit resource protection needs, standards, and procedures. Each unit commander, tenant unit agency chief or commander, or equivalent staff agency chief must ensure their resource protection program meets Air Force and DoD protection criteria. Each commander or agency chief must appoint in writing a resource protection program focal point and send a copy of the letter to the RPPM. There is no minimum grade or rank requirement, however, the person selected will work with the CSP, RPPM, and RPEC working groups. Your focal point will help you convey your program needs to the RPEC and installation commander. Chapter I of AFI 31-209 outlines additional program responsibilities.

1.6. Resource Protection Executive Committee. The RPEC is one of the most important advisory bodies on an Air Force installation. It has no rival in its responsibility or authority to advise on protecting vital resources and the installation's war fighting capability. Together, members of the RPEC develop policy and procedures for the safeguarding of installation resources. The RPEC establishes and oversees the work of any number of specialized working groups which report to the RPEC chairman.

1.6.1. Chairman. The installation commander or his deputy serves as the RPEC Chairman and determines the need, frequency, agenda, and participants of the RPEC. RPEC members should include principal deputies from major functional and support agencies. The CSP and RPPM should also attend as either members or principal advisors. Consider other US service component members, allied and foreign host nation government and military officials if applicable and deemed prudent by the chairman.

1.7. Sub-committees. The chairman convenes the various traditional working groups covered in AFI 31-209, chapter 1, and reviews their recommendations. The chairman also directs the formation of other working groups needed to support program management requirements. Actual membership composition is based on specific problems and issues. However, the chairman should consider carefully those individuals selected to chair working sub-committees. Strong managerial skills and full understanding of the current problems are crucial. Remember, recommendations and staff actions from various working groups will form the basis for RPEC decisions. And as discussed earlier, the RPEC convenes as a decision making body and so relies heavily on the staff work and research of its support committees.

Chapter 2

PROGRAM PLANNING AND MANAGEMENT

2.1. Management Philosophy. When planning for resource protection you must prioritize resources and ensure each is protected according to its value, vulnerability, and the role it plays in meeting the wing mission. Unit level planners must take basic program requirements and build local procedures which will afford the appropriate degree of protection. Each MAJCOM resource protection program manager must provide supplemental planning guidance while working closely with their RPPM to help them meet unit level protection requirements. Regardless of your position within the resource protection program, your focus must develop plans and procedures that will protect mission critical, and war fighting assets.

2.1.1. Resource protection management begins at the installation level, starting with a sound risk analysis of assigned resources. A risk analysis provides the commander with a method to rank order the installation's mission essential resources against postulated threats This analysis serves three main purposes. First, it identifies those resources, in priority order, that are most critical for mission accomplishment. Secondly, it analyzes current threats to those resources and strikes a balance between risk and the available assets (financial and physical) to protect them. Finally, it serves a the baseline for managing and prioritizing expenditures to combat those threats. This is a complex task requiring careful thought and study. The RPEC and the planners that support them are crucial to the proper development of an installation's risk analysis. The following are just some of the questions to consider when performing or evaluating the installation's risk assessment:

2.1.1.1. What is the true nature of the threat, and what is the likelihood that threat events could occur?

2.1.1.2. What is the mission of the wing, and what resources are critical to its accomplishment, and therefore require protection at all costs?

2.1.1.3. What is the logistical strength and depth of the installation and can it easily replace or repair resources?
2.1.1.4. How well can the installation physically protect its assets, i.e., response force capabilities, quality of storage structures, IDS, other equipment, location, terrain, and other factors?
2.1.1.5. How well does the installation link its manpower and financial planning with resource protection planning?
2.1.1.6. How large, trained, and equipped is the protection force? What is the probability of breaching security either internally or externally?
After proper risk assessment, you may begin the protection planning process.

2.2. Program Planning. The objective of resource protection planning is to identify resources, analyze the potential threat against them, and then develop realistic counter measures. Increasingly sophisticated methods used by both conventional enemy forces and the criminal element make this an increasingly difficult task. Limited manpower and financial assets only further enhance the challenge. In-depth protection, crime prevention through environmental design, good plan development, and the concern of all unit personnel for resource protection are the most important considerations in resource protection planning.
2.2.1. In-Depth Protection. The concept of in-depth protection calls for the careful use of barriers, lighting systems, entry control, random patrols, hardened structures, alarm systems, and the like. Multiple levels (depth) greatly increase the likelihood of detection and serve the greatest deterrence against unauthorized entry, damage, or theft. A locked safe kept in a locked room monitored by intrusion detection systems, which in turn is inside a well lit building randomly patrolled by law enforcement or owner/user personnel, is one example of in-depth protection.
2.2.2. Crime Prevention Through Environmental Design (CPTED). A relatively new concept, CPTED aims to prevent loss through facility and environmental planning. Simply put, CPTED uses smart planning to deter crime. Elimination of isolated stairwells, better use of lighting, and architectural design that emphasis openness and natural surveillance are only a few examples. Building a night depository across the street from a police station is a good example of CPTED. The military application potential for CPTED is endless and should remain a top consideration when renovating or constructing new military facilities. To apply CPTED effectively, the installation CSP must serve as a member (or consultant) of the base facilities utilization board. The CSP must review all plans for construction or major renovation of structures housing the following resources:
2.2.2.1. Weapons storage facilities
2.2.2.2. Sensitive munitions and explosives storage facilities
2.2.2.3. Night depositories
2.2.2.4. Funds facilities authorized to store more than $25,000.00 on a routine basis
2.2.2.5. Pharmacies or other facilities storing sensitive pharmaceutical substances
2.2.2.6. New dormitory and installation housing area construction
2.2.2.7. Parks, recreation areas, schools, hospitals, shopping areas, and major storage areas
2.2.2.8. Any other facilities required by the RPEC, installation commander, or CSP, which could benefit by review from a CPTED perspective
2.2.3. Plan Development. Developing sound protection plans require good decisions based on accurate information, experience and knowledge. Commanders, supervisors, and resource protection program managers must realize that they can not make every resource invulnerable. Therefore risk analysis and risk management become major planning responsibilities. Unless otherwise mandated, the decision to protect or not to protect, and to what degree, is made locally. The RPEC or designated working group is therefore the best forum for accomplishing sound installation protection planing.
2.2.3.1. General Planning Requirements. Once resources are known and risk analysis for both peacetime and wartime operations determined, the RPEC may begin actual plan development. Chapter two, AFI 31-209 contains specific areas to consider during the development of the IRPP or ISP. Review those requirements along with the mandatory physical protection/construction criteria contained in chapters three through eight of AFI 31-209 as well as applicable areas of this manual. Ideally the RPEC (or designated working group) can then determine its most urgent resource protection needs. It's understood that each RPEC determines how it will meet Air Force resource protection goals based on their installation's unique mission and threat assessment. The following illustration, referred to as the storyboard or list method, is only one of many methods proven successful in determining resource planning requirements.
Working group members begin by listing, in order of importance, the installation's most crucial war-fighting or mission essential resources. The list can contain a specific resource or an area where many resources are located. For example; munitions storage area as number one, followed by command post, finance vault, post office, NCO club, etc. Next list DoD and Air Force regulatory protection and construction/design criteria for those resources. Also list any MAJCOM or installation mandated requirements. Third, annotate resources/facilities not meeting the criteria, the areas deficient, and actions underway to correct deficiencies. Fourth, compile a priority listing of those resources or facilities needing immediate attention and outline possible solutions, either permanent or temporary. Finally, the working group recommends specific corrective action

using available manpower, construction funds, consolidation techniques, compensatory measures, or waiver/exception authority. The installation commander reviews recommendations and takes action as appropriate.
The above process is a complex time consuming task, but it's a proven method for grasping "where you are" and for determining what areas need your attention. If the threat or nature of your mission changes significantly, or a comprehensive evaluation such as the one described is three years or older, then you should consider doing one. A specialized working group chartered by the RPEC commander is an excellent choice for conducting one.
2.2.4. Personal Awareness. Strive to get everyone on the installation vigilant and concerned for resource protection. Your greatest protection challenge involves heightening their awareness and instilling a "feeling of ownership." History shows time and again that most loss, damage, and theft of military resources were wholly or in part attributable to a lack of care, concern, or awareness. Only a small percentage was the result of insufficient physical safeguards. Consequently, commanders and supervisors can make their greatest contribution to resource protection by developing an awareness and a conscious concern for security within their organizations. Getting everyone to look hard at what many take for granted, i.e., security of Air Force resources, is a complex problem that will require your full attention and imagination. Random evaluations to judge resource protection awareness may help determine the level of security awareness in a unit. Results form a baseline from which your attention and creative imagination can focus. Awareness data might come from formal anti-robbery exercises, interviews, written questionnaires, or simply watching people around you react to various situations. Awareness measurements are important in assessing where your people are in relation to that feeling of ownership we discussed earlier. Remember, vigilance and awareness of the people and things around you is perhaps the most important, and sometimes most neglected area in resource protection.

2.3. Deviations. Unless directed otherwise, the installation commander approves waivers, exceptions, and variances to nonnuclear protection standards. This authority also applies to criteria contained in DoD 5100.76. Waiver/exception authority is conditional on the requirement that major commands maintain waiver/exception information on those command facilities that do not meet baseline security requirements. Refer to chapter 4 or AFI 31-101, The Air Force Physical Security Program, for further information regarding the Air Force deviation program.
2.3.1. Procedures. After thorough assessment, and identification of compensatory measures, (if available) installation commanders may waive or grant exception to protection standards. Waivers and exceptions are processed using local procedures and chapter nine of AFI 31-209. The CSP makes waiver/exception approval recommendations to the installation commanders. The Installation commander also determines the review, disposition, and filing procedures for approved waivers and exceptions. Send a copy of each approved waiver or exception to your MAJCOM resource protection program manager.
2.3.1.1. MAJCOM Requirements. The RPPM at each MAJCOM reviews waivers and exceptions and notifies appropriate staff agencies if it appears a deficiency may hamper current, future, or contingency operations. As managers, they must help their installations correct deficiencies as soon as possible. Additional manpower, MAJCOM funding, and transfer of physical assets from other installations are just a few ways they might assist.

2.4. Resource Protection Program Reviews. AFI 31-209, Chapter 2 outlines facilities that must undergo formal resource protection program reviews. Develop inspection checklists using standards contained in MIL-HDBK 1013/1A, Design Guidelines for Physical Security of Fixed Land-Based Facilities, other Air Force and DoD publications, this handbook, and local directive. Most reviews are conducted at AA&E and controlled area facilities, however, the AA&E and controlled area designations are not the defining parameters for resource protection program reviews. Any facility can benefit from a resource protection program review. Facilities that you must evaluate (as defined in AFI 31-209, Chapter 2) are performed under the direction of the RPPM with assistance from other base agencies. When not directed by MAJCOMs, installation commanders designate, in an appropriate base security plan or supplement to this AFI, other facilities requiring resource protection program reviews and those who will perform them. As a general rule, unit personnel can do those reviews with guidance from the RPPM. Regardless of the responsible agency, commanders must notify the CSP when any facility will need an initial review as discussed in para 2.5.
2.4.1 The RPPM prepares original reports and ensures they are staffed and signed IAW with local procedures. Keep the written review in a facility resource protection folder. Maintain a folder on all facilities required by AFI 31-209, local RPEC, or other directives. Determine configuration of folders locally, but keep one copy of all initial, follow-up, and special program reviews in the folder. Other documents to store in the review folder include:
2.4.1.1. Designation letters authorizing firearm and/or fund storage
2.4.1.2 Designation letters establishing controlled areas
2.4.1.3. Letters designating controlled areas and their current unit monitors
2.4.1.4. Letters designating the storage of munitions, and storage limits
2.4.1.5. Copy of the facilities initial survey
2.4.1.6. Waivers and/or exceptions

2.4.1.7. Miscellaneous resource protection reports, i.e., anti-robbery, exercises, awareness surveys, etc.
2.4.2. The folder serves as a management tool and single point of reference for all resource protection documents, issues, questions, or problems effecting a particular facility. When reading the folder, it should identify facility deficiencies, (if any) compensatory measures, type and currency of any waivers/exceptions, when exercises and evaluations were last conducted, status of corrective recommendations, names of who key unit resource protection managers and other important information. Format, structure, and exact content of the folder is not critical. Instead, the folder must serve as a reference for making planning and program decisions. If it is not accurate or does not reflect the current status of a resource or facility, then it is of little value to you.
2.4.2.1. Disposition and Review. Store, safeguard, review, and maintain resource protection folders IAW local procedures and AFM 37-139, Records Disposition Schedule.. Folder contents are for official use only, therefore, treat and safeguard them as sensitive information. Installation commanders may classify selective resource protection documents, if their content, or collective sum, could reasonably jeopardize classified assets or operations. Refer to the installation information security program manager for guidance.

2.5. Types of Review and Their Requirements. There are four types of resource protection and controlled area reviews: initial; follow-up; special; and supplemental. Initial and follow-up are coordinated by the RPPM. Unit commanders direct special and supplemental inspections. These surveys are not intended to replace the guidance issued in other Air Force instructions or other required inspections or surveys (for example, safety and storage inspections required by other federal and Air Force directives). Facilities containing classified material are inspected under AFI 31-401, Managing the Information Security program, and DoDR 5200.1R, Information Security Program Regulation. For Sensitive Compartmented Information (SCI) facilities, refer to DOD S-5105.21-M-1, Sensitive Compartmented Information Administrative Security Manual, and AFM 14-304, The Security, Use, and Disposition of Sensitive Compartmented Information (SCI).
2.5.1. Initial Survey. An initial survey is the first detailed survey made on a facility to establish protection requirements. It outlines areas that you must address during pre-contract meetings, design phases, and construction or remodeling. It includes a complete analysis of the facility, to include its operation, physical protection hazards and deficiencies. The actual “initial report” is completed after the last review is completed, but before a facility opens or new operations begin. You may conduct this evaluation separately or as part of a larger inspection attended by representatives from civil engineering, base contraction, fire department, base safety, and other agencies that typically “certify” a facility ready (or not ready) for use. The initial review process can cover several years with the RPPM conducting many partial inspections and attending numerous meetings, negotiation conferences, and the like. Consequently, the finalized initial review report may contain many attachments detailing various planning and inspection phases, negotiations, meetings, etc. The RPPM completes the initial review and forwards it to the CSP. The report should contain a list of all significant discrepancies related to security and an overall evaluation of the facility’s fitness for operation as it pertains to the protection of its resources. The CSP reviews the report, attaches a final recommendation, and forwards it to the installation commander for action. The installation commander reviews the report, takes appropriate measures, and returns the report for permanent filing with the RPPM or designated office.
2.5.2. Follow-up survey. Conducted annually from the date of the initial survey, or as needed, to verify that agencies have corrected discrepancies and deficiencies from earlier inspections. The installation commander or CSP review all annual follow-up inspections. Staff and review other follow-up reports, such as those to review the correction of deficiencies, minor construction modifications, etc., according to local policy.
2.5.2.1. At times the difference between an initial and follow-up survey can be confusing. For example, conduct an initial survey of a newly built command post before command post operations move into the facility. Likewise, if base operations then moved into the old command post facility, it would (assuming base operations is a controlled area) require an initial survey to see if the old command post facility meets construction and security standards required for base operations even though both facilities (old base operations and old command post) have initial and follow-up surveys on record. Guidelines from the installation commander and CSP will help determine the appropriate survey.
In addition to special considerations cited above, follow the guidance in chapter 4 when conducting controlled area surveys.
2.5.3. Special survey. The MAJCOM, installation commander, or RPEC may direct special surveys at any time. Unit commanders may also direct special surveys anytime protective deficiencies exist in their operations or when a change occurs in the facility that alters its protective capability. Conduct special surveys with unit personnel or jointly with the RPPM. When support is needed from the RPPM forward a request letter to the CSP. The letter should cover the following:
2.5.3.1 Scope of the survey, its purpose, and the area to survey
2.5.3.2. Type or class of resources affected and any potential hazards
2.5.3.3. Current deficiencies relevant to the requested survey
2.5.4. Supplemental surveys. The owning unit conducts supplemental surveys at regular intervals until completion of all discrepancies noted during initial, annual, or special surveys. Perform supplemental surveys separately or incorporate into unit self-inspection programs. Conduct, document, and file supplemental surveys according to local policy.

2.6. Minimum Protection Standards. During initial and follow-up resource protection and controlled area reviews, the survey team chief (usually the RPPM) must balance many considerations. Not every facility can meet every protection standard. Your imagination may well prove your greatest asset when trying to strike a balance between what exists, what is required, and what compensatory measures are feasible to ensure resources are not compromised. In addition to identifying deficiencies you should recommend possible alternatives and solutions. Remember, the unit and installation commander will rely heavily on your judgment and recommendations. Clearly identify deficiencies and the action necessary to correct or counter them. Examples of some discrepancies are: 1) indications of inadequate boundary or barrier systems (because of poor fencing, lighting systems, unprotected windows and the like);

2) evidence that indicates trespass of the building or area exists and is a matter of routine or an accepted practice; 3) indications that circulation control and the checking of entry credentials (when required) is inadequate; 4) a lack of security consciousness of those working in or around high value resources; 5) poor resource protection education and motivation; and 6) a lack of supplemental surveys or sense of urgency to correct previously identified deficiencies

Each of the above program deficiencies has its counter, i.e., well secured facilities, strong motivational programs, and positive sense of awareness and security on the part of unit personnel. Highlight such observations in reports and cross-flow to other units, which can help them improve their programs.

2.6.1. Minimum survey requirements. As a minimum, surveys should evaluate the following areas:

2.6.1.1. Unit methods for training personnel in circulation control procedures and protection awareness

2.6.1.2. Unit security operating instructions pertaining to controlled areas, or high value storage areas

2.6.1.3. Procedures covering key control, entry procedures, circulation control, and security checks

2.6.1.4. Compliance with construction standards as they relate to security and potential penetration, i.e., wall thickness; lock and door grades; vent, window, and crawl space access, alarm installation, etc.

2.6.1.5. Are all required facilities and equipment installed?

2.6.1.6. Are they in good condition and repair?

2.6.1.7. Are procedures established for routine and emergency maintenance?

2.6.1.8. If applicable, does the IDS function properly and are alarm systems tested IAW AFI 31-209?

2.6.1.9. Are facilities built to specifications required by AFI 31-309 and Mil-Hdbk 1013/1A, and other applicable construction references?

Do procedures exist for receiving, controlling, accounting, and transporting sensitive or high value items?

2.6.1.10. What is the potential for unauthorized access through attics, boiler rooms, basements, air vents, crawl-spaces, etc.

2.6.1.11. Compliance with written procedures and overall security awareness of personnel working in the controlled area

2.6.1.12. If the facility deals with classified material, its compliance with requirements contained in AFI 31-401 and DoDR 5200.1R

2.6.1.13. Compliance with MAJCOM and local controlled area and resource protection requirements

These are just some of the areas you need to access when conducting physical security surveys. Incorporate them into MAJCOM or local checklists.

2.7. Documenting Controlled Area Surveys. Responsible commanders must notify the CSP when a facility will require an initial controlled area survey. Generally, staff and brief the activation of new controlled areas, or significant changes to an existing controlled area, well in advance as they require installation commander designation and approval. Brief controlled area changes to the installation commander at the next scheduled RPEC meeting. When under time restraints or when a full RPEC meeting is not warranted, the responsible commander, controlled area manager, or RPEC working group should brief the installation commander in a separate meeting. When controlled area establishment is warranted, the installation commander directs the CSP to staff the initial controlled area review. Controlled area surveys (either initial or follow-up) often require a degree of expertise in the area of physical, industrial, and information security. Consequently, members of the security police resource protection branch are often best suited for performing the physical (and administrative if so designated) portion of the review.

2.7.1. The survey report should focus on the proper use of signs, operating instructions, and physical procedural compliance. Equally important are the intangibles such as motivation, awareness, attitude, and the overall security consciousness of personnel working with resources. The report should cover the areas discussed in paragraph 2.6. of this handbook. When complete, forward the report to the CSP for review.

2.7.1.1. The CSP reviews the report with close attention to the seriousness of discrepancies (if any) and the report's summary recommendation to the installation commander. Local policy determines who signs survey reports, but the report should provide the installation commander with a final summary or recommendation. In it, state the overall fitness of the facility to protect its resources and continue operations as designed. When there are serious deficiencies that threaten resource security brief the installation commander immediately, do not wait for the normal staffing process. Forward written reports to the

installation commander who in turn annotates review of the report, takes appropriate action, and forwards the original to the RPPM for inclusion in the facility file. Additional copies and staff action is determined locally.

2.8. Frequency of Reviews. AFI 31-209 chapter 2 directs the minimum standard of initial and follow-up reviews for some categories of high value or mission essential resources. Refer to that AFI for additional information. MAJCOMs or installation commanders determine other program review requirements. Generally these are areas containing significantly important resources such as weapons, munitions, drugs, funds, high cash value items, and other material the MAJCOM or installation commander believe would benefit from a formal review and assessment. The installation commander should review all the factors significant to their particular resources, their mission and location when determining the need and frequency of additional resource protection program reviews. Note: As a general rule, the above guidance does not apply to a sensitive compartmented information facility (SCIF) inspected, certified, and accredited under USAFINTEL 201-1, The Security, Use, and Dissemination of Sensitive Compartmented Information. Refer to that publication or ists successor document and local support agreements for additional guidance.

2.9. Resource Protection Exercises. Determine policy for resource protection exercises locally. AFI 31-209, chapter 2 identifies requirements for anti-robbery exercises. The content of that AFI and chapters one and two of this manual provides the information necessary to determine the number, type, and focus of exercises for your installation. The goal is to provide the greatest degree of protection, for the greatest number of resources, for the least cost. Success requires assessing and managing risk while prudently applying cost effective protective and awareness measures. This is a responsibility for all commanders having assets that require protection under the Air Force Resource Protection Program.

2.10. Summary. Good resource protection management requires constant attention, innovation, and smart fiscal management to meet Air Force resource protection program objectives. Installation commanders and their planners can’t meet those objectives without everyone’s full support. Therefore, personnel at every level must take an active role in resource protection planning and management. Then, and only then can we ensure a safe and secure environment for our Air Force resources.

Chapter 3

EQUIPMENT AND FACILITY STANDARDS

3.1. Overview. This chapter outlines how to apply security criteria and protection standards for equipment and facilities that require protection under the Air Force Resource Protection Program. The protection of these assets is best accomplished through a combination of manpower, effective controls and procedures, and the appropriate level of awareness, surveillance and/or physical barriers. Installation commanders use the CSP, RPEC, and specialized working groups to help them determine the right combination necessary given their mission, threat, and local requirements.

3.1.1. Consider the guidance in this chapter against the specific resource protection climate and mission of your base. The following are just some of the many things to consider:

3.1.1.1. Location of your installation, its mission and the type of resources assigned

3.1.1.2. Current and projected wartime threat vulnerability and the nature and scope of the wartime mission. For example, do assigned resources deploy out or do vulnerable assets stage, transit, or deploy in? What is the anticipated reaction of the local population during your wartime contingencies?

3.1.1.3. Size, training, and capability of local security forces

3.1.1.4. Content of your local terrorist threat assessment and the documents discussed in para 1.3.2 of this manual

3.1.1.5. Geography and physical lay-out of the base

3.1.1.6. Quality of various structures and existing protection standards. For example, outdoor open storage of munitions versus availability of hardened munitions bunkers.

3.1.1.7. Availability of friendly forces and degree of support from local communities, governments, or host nation

These factors are just some of the many that will determine your resource protection needs. Keep them in mind when reviewing the protection guidance that follows.

3.2. Installation Perimeter Fencing. A fence serves as a legal and physical demarcation of an area or boundary. Since a fence serves as a deterrent to the casual intruder and legal definition of an area generally excluded to the public, consider it a primary aid for resource protection applications. AFI 31-209, requires installation perimeter fencing unless specifically waived by the installation commander. Before waiving or removing existing perimeter fences, the installation commander

must carefully weigh all the factors, to include potential value of the fencing during war-time or special contingency operations. Some installations, because of topography, size, or type of mission, do not lend themselves well to fencing, however, those locations are the exception.

3.3. Controlled Area Fencing. The installation commander determines the fencing of controlled areas. Consider the factors outlined in para 3.1.1. and AFI 31-209 when determining the need for controlled area fencing.
3.3.1. If an area or resource you want to protect does not lend itself to the principle of "deterrence at the area boundary" or "surveillance of the area boundary" then fencing is not effective and probably unnecessary.
3.3.2. When fencing is practical and the importance of the resource is significant, construct fencing in accordance with standards published in MIL-HDBK 1013/1A, and chapter 5 of DoD 5100.76-M.

3.4. Flight Line Fencing. The installation commander determines the need for fencing the flightline. Consider cost and maintenance factors against manpower savings (reduced patrols and entry controllers) and any security enhancement gained by the barrier created by fencing. Installation commanders must carefully consider many factors to include those outlined in para 3.1.1. Of key importance is the geography and layout of the flightline area, resources and mission assigned, and the nature of anticipated wartime operations. Installations having significant combat support roles in which large numbers of resources or aircraft will transit or stage from the installation must strongly consider the value of flightline fencing and the entry control it affords. Do not arbitrarily remove existing flightline fencing without careful consideration and approval by the installation commander.

3.5. Fencing for Sensitive Compartmented Information Facility (SCIF). Fencing requirement for these facilities are established by DIA DAC 2A. The owner/user must address and document the standards given them by DIA DAC 2A in their facility's resource protection folder.

3.6. Fencing of Munitions Storage Areas. Fencing is required for areas designated for the storage of category I and II nonnuclear munitions. Fencing is optional for category III and IV storage facilities and is determined by the installation commander or RPEC.

3.7. Other Fencing Applications. Installation commanders are responsible for a base environment that meets reasonable public safety standards. These standards, and the definition of "reasonable" varies depending on local jurisdiction. Commanders must ensure certain areas and "attractions" that, by their very nature, make them inherently dangerous to the public are protected from reasonable access. An unprotected swimming pool adjacent to the base housing area would likely not pass a judicial test for "reasonable public safety" and thus leave the Air Force vulnerable to litigation should a child drown or become injured. Security fencing and the posting of warning signs have proven both an effective safeguard, and in most cases, clear evidence of a prudent and reasonable public safety measure. Ensure the staff judge advocate (SJA) is involved in such decisions.
3.7.1. The following are some areas to evaluate for fencing or other appropriate barrier measures:
3.7.1.1. Communication and radar facilities Fuel storage areas
3.7.1.2. Fuel storage areas
3.7.1.3. Water towers
3.7.1.4. Munitions storage areas
3.7.1.5. Hazardous material holding areas
3.7.1.6. Swimming Pools
3.7.1.7. Electrical relay, transformer stations
3.7.1.8. Engine test sites

The above are just some hazardous areas found on a typical military installation. Fence, secure, or place such areas and others in such a manner that they do not pose a reasonable threat to public health and safety. The installation commander should direct the RPEC, with assistance from the SJA, to seek out and evaluate all such potential areas. Fence those deemed appropriate and post warning signs to ensure the protection of resources as well as the public safety.

3.8. Lighting Requirements for Resources. Lighting is invaluable in helping to protect resources. If unmanned, you must light the exterior doors and windows of storage magazines, and all facilities containing Category I and II AA&E during hours of darkness and during other times of decreased visibility. Exception: Lighting is not mandatory for facilities located in restricted areas or patrolled Nonnuclear Munitions Storage Areas (NMSA). All other lighting, unless specifically required by other directives, is determined locally and is the responsibility of the unit responsible for the facility housing the resources.

The base RPPM will assist owner users in determining their need for installing or modifying existing lighting systems. Address lighting needs in owner/user resource protection surveys.

3.8.1. Engineering. Individuals involved in developing resource protection measures must ensure recommendations and requirements are reviewed by installation civil engineers. Ensure all lighting components meet standards outlines in MIL-HDBK 1013/1A, AFH 32-1084, Standard Facility Requirements Handbook, and their associated references.

3.9. Backup Power Requirements for Resources. Provide key command and control centers and resources of special sensitivity with a backup power source.

The law enforcement desk, SCIFs (as required by DIA DAC 2A), and facilities for Category I or II AA&E resources must also have backup power, or appropriate countermeasures when commercial power is lost. The RPEC determines which base facilities require emergency backup power, and prioritizes construction and funding projects for those that do not meet standards. Facilities requiring backup power must comply with the requirements in AFI 31-209 Chapter 3.

3.9.1. We encourage you to keep your MAJCOM Resource Protection Program Managers informed about unfunded resource protection requirements. MAJCOMs may transfer excess command requirements and assets to meet installation needs.

3.10. Intrusion Detection Systems (IDS). The use of IDS is a vital part of protection systems. Reliable IDS used with timely alarm assessment and response is invaluable to your protection program.

3.10.1. The Joint Service Interior Intrusion Detection System (J-SIIDS) is the Air Force approved IDS for resource protection activities. Air Force installations should continue using this approved system where possible. Each installation using J-SIIDS must ensure they forecast their annual J-SIIDS support requirements. Forward this forecast to the Defense Logistics Agency through normal supply channels. Forecasting requirements is a owner/user responsibility, however, each RPEC should consider appointing someone knowledgeable in J-SIIDS to oversee development of the annual forecast. Report serious shortages and program deficiencies to your MAJCOM Resource Protection Program Manager. When followed, the guidance in this chapter, and that found in AFI 31-209 Chapter 3 will ensure adequate J-SIIDS support (hardware, software, repair, parts, etc.) for your systems.

3.10.1.1. If J-SIIDS does not meet the installation's resource protection requirements other solutions are available for consideration. Advanced Entry Control Systems(AECS) and Integrated Commercial Intrusion Detection Systems(ICIDS) are also available. Commercial Off The Shelf (COTS) systems are also an alternative. If considering a COTS IDS, give special consideration to ensure long term supportability and maintainability is provided in the initial Statement of Work (SOW).

3.10.1.2. The RPEC should consider setting up a sub-working group when reviewing and buying IDS. Include civil engineer, security police, communications, and contracting personnel for technical oversight. Additional IDS acquisition guidance is provided in AFH 31-104, The Air Force Sensor Handbook.

3.10.2. Use of Base and Installation Security Systems (BISS). In certain applications, BISS components may provide a better alternative. When J-SIIDS components are not available, BISS components may replace or augment J-SIIDS systems. Use TO 31-S9-1-101, J-SIIDS Selection and Application Guide, to decide which group or groups of components are best suited for a particular application or substitution. Fully consult the RPPM and base civil engineer before using BISS in place of J-SIIDS applications or components.

3.10.3. IDS standards for SCIF: Director of Central Intelligence Directive (DCID)1/21 contains IDS protection standards for SCIFs. The guidance in para 3.9. applies to the use of IDS in SCIFs.

3.10.4. Use only approved IDS systems in resource protection applications. However, the installation commander may authorize use of non-standard systems when J-SIIDS support proves unavailable or inappropriate for the application required. Your MAJCOM RPPM can assist you in procuring J-SIIDS equipment (in the case of shortages) or in your selection of a non-standard system. Coordinate non-standard system needs through your MAJCOM RPPM prior to procurement obligation. When procuring non-standard systems strictly adhere to the following procurement guidelines:

Note: Plan, procure, and use IDS systems through the resource protection survey system. This is accomplished jointly by security police, civil engineer and the owner/users.

3.10.4.1. Lease rather than purchase commercial IDS systems unless comparative cost analysis indicates other procedures are significantly more cost effective. Units that purchase commercial systems may limit their options and flexibility as future Air Force and DoD sponsored systems are developed and procured.

3.10.4.2. Ensure intercomponent cabling in commercial IDS is compatible and interoperable with DoD systems. Leasing arrangements must include a provision for government retention of all component wiring or cabling associated with the commercial IDS after termination of a lease agreement.

3.10.4.3. The contractor, base civil engineer, and a representative from the communication squadron must certify the commercial IDE is functionally compatible and interoperable with components of J-SIIDS and/or BISS to connect to, or used with, the commercial equipment.

3.10.4.3.1. Roughly measure equivalency by comparing the commercial system's performance characteristics against J-SIIDS capabilities in TO 31S9-1-101. In such cases, the burden of proof (and liability) regarding claimed performance rests with the contractor. Give special considerations to IDS "equivalency" if components in Annex B of D/CID 1/21, Director, Central Intelligence Directive, are not readily available. Refer to D/CID 1/21 for specific details.

3.10.5. IDS for Army/Air Force Exchange Service (AAFES) Facilities: The management of IDS for non-DoD sponsored agencies require negotiation and close coordination between AAFES management and installation commanders. IDS required by the installation commander (in excess of AAFES management directives) are procured, installed and maintained without cost to AAFES. However, negotiate system upgrades, and general IDS improvements beyond AAFES requirements, which enhance the protection of AAFES resources, in good faith between AAFES and installation management. Cost sharing and joint ventures are authorized and encouraged.

3.10.6. System Characteristics: Installation IDS must maintain minimum protection standards. The following standards apply to all IDS systems:

3.10.6.1. Flexible, that is, used to protect large or small areas with little modification and cost difference.

3.10.6.2. Able to register any malfunction positively, and have a malfunction alarm rate that does not exceed one malfunction per each 24 hours for each sector or protected zone.

3.10.6.3. Possess both audible and visual annunciation capabilities, and a line fault indicator if the system fails. Must have on and off switches (not located at the annunciator panel) and access or secure switches located within the alarmed area.

3.10.6.4. Must have good quality, dedicated communication cable pairs for transmission of the encoded system.

3.10.7. Responsibilities for IDS Management: The security police monitor IDS and duress alarm systems. Unless under separate civilian contract, the base civil engineer installs, modifies, and maintains IDS and duress systems for resource protection. DCID 1/21 establishes requirements, and DIA DAC 2A approves IDS for USAF SCIFs as part of the accreditation process. Where possible, fully integrate SCIF IDS into the base IDS program.

3.10.7.1. Modification to installation IDS requires civil engineer and CSP approval.

3.10.8. IDS Annunciator Terminal: All resource protection alarms must annunciate at a 24 hour manned facility such as the law enforcement desk (LED), main gate, or separate alarm monitoring facility. All facilities serving as IDS annunciator terminals must have a duress alarm that terminates at the LED and a primary and backup form of communication with another manned facility.

3.10.9. Types of IDS. The types and availability of IDS are outlined in supply procurement standards and AFH 31-101. System performance criteria of a technical nature, beyond the scope and practicality of this publication, are also contained in AFH 31-101. You should consult AFH 31-101 during IDS review or procurement process. Virtually all commercial systems are a variant of, or work similar to, the DoD standard components found in J-SIIDS or BISS. Since some equipment is not compatible with all applications (for example ultrasonic noise detectors in high noise areas), a familiarity with the types and the application location characteristics is essential.

3.10.9.1 Penetration Detection. There are two types of penetration detection sensors:

3.10.9.1.1 Complete Penetration Detection. Detects penetration attempts through doors, windows, and surfaces such as walls, floors, and ceilings. This is often the outer most, or "early warning" level of alarm.

3.10.9.1.2 Boundary Detection. Detects penetration attempts through a facility boundary such as vents, crawl spaces, windows or doors. It differs from complete penetration detection in that floors, walls, and ceilings, or other non-existing openings are not protected. Boundary detection alone is not sufficient for unmanned facilities requiring full IDS protection.

3.10.9.2. Motion Detection. This type of detection is also called volumetric or space detection. It is the detection of a person's movement inside a protected area. This is a highly effective and complementary alarm system when installed in conjunction with, but independently of, penetration detection systems.

3.10.9.3. Point Detection. Detects attempts to remove protected items within a secure area, such as documents in a wall safe or locked filing cabinet. This is the inner most level of intrusion detection and is the last opportunity to detect intrusions. Point detection gives the least warning in terms of reaction time for response forces. Innovation and imagination are key concerns in the application of point detection, as intruders reaching this point undetected are likely skilled and well versed in breaching detection systems.

3.10.9.4. Duress Alarms. The duress alarm is not a component of the three IDS previously discussed. Duress alarms are effective in manned facilities where unauthorized personnel may force surrender of protected resources. Facilities requiring duress alarms are identified throughout this handbook and AFI 31-209. The installation commander or RPEC determine duress alarm requirements beyond requirements found in AFI 31-209.

3.11. System Performance. Each base having IDS must have an effective maintenance program. Installation procedures or maintenance contracts must provide for timely emergency response when IDS systems fail. Local policy or operating instruction will determine when emergency maintenance response is required. The number of inoperative alarms, type of resources now vulnerable, and availability of owner/user personnel to man facilities are key considerations.

3.11.1. Owner/user personnel responds to monitor facilities with inoperative IDS. Facilities discussed in chapter 6, para 6.5, and chapter 5, para 5.12. require
either mandatory manning, installation of portable IDS, or other measures that equal or exceed the detection afforded by the facility's IDS were it functional. Installations using IDS should develop local procedures to ensure rapid and full protection of facilities when their intrusion detection systems become inoperative.

3.12. IDS Protection Requirements. Protect all IDS against tampering or bypassing.
3.12.1. Locate IDS control panels inside a manned or alarmed area. Lock and alarm cable and switch boxes with tamper or intrusion detection switches.
3.12.2. Transmission Lines. Intruders may attempt to defeat IDS by way of transmission lines, so consider affording special protection to them. All IDS must include some form of line supervisory capability. Simple line voltage, current variance, and line resistance systems offer the least protection. Data transmission signals using random pulse signal generators offer more protection, and within these systems are various degrees of complexity and surety, depending on the signal logic used. The RPPM in coordination with base civil engineers, communications personnel, contractors, or others as appropriate, determines the sufficiency and type of line supervision to use. Consider theft/loss vulnerability and value of the protected resource when determining the level of sophistication (and cost) of line supervision. Also review protection criteria outlined in chapters 4 and 5 and their associated references.
The base RPPM and civil engineer can assist in determining suitability of current or proposed systems.
Note: Protect Information compiled concerning type of IDS and their possible vulnerability as sensitive information and control appropriately.
3.12.3. IDS Monitor Responsibilities: Train alarm monitors to understand the system they monitor, including basic operation and fault isolation. Owner/user management is responsible for ensuring proper training of personnel and contractors monitoring their IDS. The CSP assumes this responsibility for all security police acting as alarm monitors. The base RPPM can assist you in developing local training criteria for alarm monitors.
3.12.4. Alarm Test Requirements: Unless determined otherwise by the RPEC, the CSP develops alarm testing procedures for installation alarm systems. Test procedures must cover all aspects of the alarm system. This includes each sensor, switch, duress activator, or other devise capable of transmitting an alarm to the alarm monitor. Evaluate alarm sensitivity, thresholds, and possible voids in volumetric or interior detection coverage during the test. Careful planning and scheduling with facility custodians is necessary to ensure full and adequate testing of alarm systems. Installations with large numbers of alarmed facilities should consider scheduling some tests during weekend and non-duty hours. The CSP may publish an alarm test schedule identifying when and how often to perform the tests to prevent overload of the alarm monitor and to ensure they conduct thorough tests. In addition, the following is required:
Note: Conducting alarm tests is an owner/user responsibility. The CSP develops initial procedures and acts as a facilitator. Owner/user personnel must ensure full compliance with CSP and RPEC testing requirements. Failure to meet alarm testing criteria is a matter of serious concern which you should report to installation leadership.
3.12.4.1. Conduct tests outlined in 3.12.4. quarterly unless the RPEC or other publication establishes more stringent standards. AAFES and Defense Commissary Agency (DECA) follow procedures published by their respective management headquarters.
3.12.4.1.1. The base civil engineer or contractor conduct tests of switch boxes, control panels, and other line supervision features designed to detect power interruption and/or tampering. Test those systems during routine maintenance or service, and at least every six months. The owner/user must document the number and location of their systems requiring civil engineer testing and ensure they perform appropriate evaluations.
3.12.4.2. Document alarm tests on any Air Force General Purpose Form, locally devised form, or an approved Air Force automated computer system. Maintain alarm test logs, to include automated records, for 90 days or longer as determined by the CSP.
3.12.5. Use of Alarm Verification Codes: When alarmed facilities are entered, use a locally devised identification verification or duress code prior to allowing entry. These local procedures must have adequate internal and external security controls. Change codes, matrix cards, duress words, and other similar information at regular intervals or whenever compromise is suspected .
3.12.5.1. The CSP develops and distributes the codes. Use computer generated codes where possible, and designate the codes "For Official Use Only." Change codes IAW guidance established by CSP.
3.12.6. Documentation of Facilities Opening and Closing: The alarm monitor must record the opening and closing of each alarm facility. Enter the name and grade (or title) of the caller, the date and time of the call, the name or building number of the facility to open or close, and the time the facility was opened or secured. Also annotate the name of the alarm monitor that authorized the opening or closure. The alarm monitor should refer to the opening and closing record as a monitoring tool to ensure facilities opened are later secured. Make the record of opening and closing a official file and maintain IAW local

procedures and AFM 37-139. If using automated systems to document opening and closing of facilities, ensure the automated record records adequate information concerning the facility, date, time, and persons conducting the transaction. File automated records IAW local procedures and AFM 37-139.

Chapter 4

CONTROLLED AREAS

4.1. Controlled Area Philosophy. Tracking, controlling, and managing the many resources contained on your military installation can become overwhelming. One tool which will help you simplify that task is use of controlled areas. A controlled area is a legally defined area, which by virtue of the resources contained therein, requires special entry and access controls. Only authorized personnel, usually designated by a unit commander, have access to controlled areas where inventory, accountability, and control over high value items is more stringent than in other areas. Unit commanders evaluate their resources and determine which areas, if any, merit controlled area status. The installation commander is the approval authority for establishing controlled areas. Remember, not all areas qualify for controlled area status. In fact, consider only resources in areas judged mission essential or those containing pilferable, high value items. Although controlled areas afford greater accountability and control, they can also inhibit access and hinder day to day operations if unwisely used. Do not set up a controlled area as substitute for positive circulation control. Instead, use a controlled area as an additive to complement existing security measures. However, if an area has sound security, good circulation and entry control features, and does not need the legal boundary provided by a controlled area designation, then a controlled area designation is probably not necessary. Unit and installation commanders should consider the following when determining when to establish a controlled area.

4.1.1. Unit location and current threat assessment

4.1.2. Number and clearance level of personnel requiring access

4.1.3 Existing internal security, physical safeguards, and floor plan

4.1.4. History of losses, damage, or theft

4.1.5. Value, cost, and uniqueness of the material or its criticality to mission accomplishment

4.1.6. Hazard or public safety concern

4.1.7. Controlled Area Manager. We recommend that each installation have a single point manager for installation controlled areas. The manager assists the CSP and installation commander with staff actions necessary to quickly and accurately review controlled areas. The manager should develop local checklists to evaluate installation controlled areas and the people who work in them.

4.2. Controlled Area Elements. The areas discussed in the preceding paragraph are just some of the issues you might evaluate when considering controlled area designation. The following identifies essential elements to any controlled area:

4.2.1. The installation commander formally establishes controlled areas in writing

4.2.2. Proper marking of the area boundary.

NOTE: The RPEC determines when to initiate or add physical barriers, lighting, or other security measures. Base this decision on the analysis of the risk management principles discussed in this handbook.

4.2.3. Written operating procedures to regulate entry into the area for internal circulation control and protection of resources. Coordinate these procedures through your CSP.

NOTE: The procedures must cover normal as well as increased security and emergency operations.

4.3. Establishing Controlled Areas. The designation “controlled area” carries the same legal and moral restrictions as a physical barrier. Unless physical barriers are specifically required, the actual effectiveness of a controlled area may depend entirely on the security awareness of the people working in it.

4.3.1. You may establish a controlled area inside a restricted area, and vice versa.

4.3.2. If an area is temporarily designated as a controlled area, the installation commander must specify the precise period, i.e., days, weeks, or months. Mark the boundary with temporary markers such as rope, fencing, or stanchions. If a barrier is already present such as existing fence, walls or buildings, then the posting of controlled area signs is satisfactory.

4.3.3. Ensure local directives designate permanent controlled areas by building number or name of the area involved. However, your local procedures should not include detailed directions or other information about your controlled areas that might aid terrorist, criminal, or dissident elements. Properly post and clearly define all controlled area boundaries.

4.3.4. The owner or user designates in writing a controlled area monitor and informs the base RPPM. The monitor manages programs and coordinates protection requirements needed to support the unit's controlled area(s).

4.4. Controlled Area Surveys. The term "controlled area survey" is synonymous with "resource protection program review." They are one and the same except controlled area surveys involve only controlled areas and place greater emphasis on the security awareness of personnel within these areas and identify how entry and circulation within the area is controlled. Both surveys review the physical layout and structure of the facility, security standards, and the overall protection afforded the resources. When conducting controlled area certifications and surveys follow the inspection guidance in chapter 2 of this AFI along with the additional controlled area inspection criteria covered in this chapter. Remember, all controlled areas containing funds or property that would otherwise require a resource protection program reviews (as defined in AFI 31-209, chapter 2) must, as a minimum, receive initial and annual controlled area surveys. The RPPM with the assistance of other base support agencies conducts controlled area surveys mandated by AFI 31-209. When not directed by MAJCOMs, installation commanders designate, in an appropriate base security plan or supplement to this AFI, other controlled areas requiring surveys, their frequency, and the agencies responsible for conducting them. As a general rule, unit personnel can perform those surveys with guidance from the RPPM. Regardless of the responsible agency, commanders must notify the CSP when any new controlled area is established and when they will perform an initial survey. Refer to chapter 2, paragraph 2.6. for further guidance. Conduct controlled area surveys in the same manner as resource protection surveys with additional emphasis in the following areas:

4.4.1. Unit security operating instructions pertaining to controlled areas

4.4.2. Procedures covering key control, entry procedures, and security checks

4.4.3. Overall security awareness of those working in the controlled area and the circulation control of those moving within the controlled area

4.4.4. Internal unit evaluations and exercises used to gauge the security fitness of controlled areas

4.5. Entry to Controlled Areas. The authority to enter a controlled area comes from the installation commander, who may delegate this authority. There are two basic qualifications for entering a controlled area: qualification and authority.

4.5.1 The installation commander determines basic entry qualifications and publishes them in the ISP or local directive. However, in some instances, higher headquarters directs entry qualifications such as for SCIF and some communication facilities. Balance the need for stringent entry qualifications against normal operational requirements and the sensitivity of protected resources. Basic qualifications can range from local file checks to in-depth special investigations.

4.5.2. Authority to enter a controlled area. The installation commander grants authority for people to enter controlled areas. However, this generally doesn't apply to SCIF entry which is governed under USAF INTEL 201-1. Refer to that publication or its successor document and local agreements governing entry into SCIF facilities.

4.6. Entry Control Techniques. The installation commander develops entry control measures for controlled areas. These measures can range from personal recognition to use of controlled area badges, third party authentication, sign/countersign, or any technique the installation commander deems appropriate.

The installation commander should approve and publish entry control measures in the ISP or other base level document.

NOTE: Do not publish detailed working procedures of entry authentication systems unless properly safeguarded or, if necessary, classified.

4.7. Controlled Area Entrances. Owners or users control entry to their areas unless the installation commander specifically assigns entry control responsibility to another agency such as security police or a civilian guard contractor. Keep controlled area entrances to the minimum necessary for safety and operational control. Where needed, install adequate physical safeguards such as fences, gates, and window bars, to deny entry to unauthorized personnel. Balance these physical safeguards against IDS (if any), location and response time of security forces, lighting situation, current threat and other factors.

4.7.1. Except when a sign would tend to compromise the security of a controlled area, post controlled area signs in conspicuous and proper places. For example, post signs at usual entrances on perimeter fences or boundaries to an area. Signs are not required for camouflaged areas in a tactical field condition.

4.8. Establishing Controlled Area Free Zones. The commander responsible for a controlled area may establish free zones. Free zones are usually established during construction projects or similar activities of a one-time nature occurring in a controlled area which make the use of escorts impractical. In such cases, set up a free zone and allow entry to the project work area at a designated point on the boundary. Ensure you coordinate the establishment of free zones with the security police, and other necessary work centers. Refer to AFI 31-101 for additional free zone construction criteria.

4.8.1. When using free zones, commanders must evaluate the need for and where necessary, introduce additional compensatory measures to ensure the security of property and resources contained in and around the free zone area.

Roving patrols, temporary barriers, additional security checks, or simply a heightened awareness on the part of those working in the controlled area may suffice. Commanders determine appropriate levels of additional security.

4.8.1.1. Make protection for the free zone boundary equal to that given the controlled area boundary. The organization or agency most associated with the project should maintain surveillance over the free zone boundary as determined by the commander responsible for the controlled area. Close the free zone and secure the controlled area after normal work hours.

4.8.1.2. Establish corridors to and from entry points in the controlled area boundary to help move equipment and personnel. Commanders responsible for the controlled area containing the free zone determine who performs entry control and how entry is controlled. If the free zone opens to the exterior of the controlled area you may use the contractor, owner, or user personnel to provide entry control, but ensure only persons with a right and need enter the controlled area. The commander also determines the method of identification used to authorize entry into the free zone when entering from the exterior boundary of the controlled area. You may use personal recognition, entry authority list, base entry ID card, or other localized method. Also, consider removing sensitive resources from the free zone area.

4.8.1.3. When you can not establish a corridor between the free zone and controlled area boundary, set up local procedures to escort people to and from the interior free zone area.

4.9. Controlled Area Badges. The installation commander or RPEC determines when to use controlled areas badges to identify persons authorized entry into controlled areas. Develop written instructions governing the control, issue, accountability, inventory, and security of the badges. Use the AF Form 2586, AF General Purpose, or locally devised form and badge for the initial issue and any mass reissue of the badges. The installation commander or RPEC determines which agency on the installation has responsibility for administering and managing the program. As a general rule, adopt the same administrative procedures that apply to the issue and control of restricted area badges for the controlled area badge program.

4.10. Use of Restricted Area Badges in Controlled Areas. The installation commander or RPEC determines if restricted area badges are authorized for use when entering controlled areas. This determination is based on many factors which you must weigh carefully. Some appropriate instances to use restricted area badges as controlled area entry authority are: 1) people who must transit through, or work in a controlled area located inside a restricted area; 2) people who must work in controlled areas which routinely become restricted areas during certain periods; 3) inspectors, visitors, or guests may use home station restricted area badges to enter controlled areas when approved by the installation commander and outlined in a local procedure, plan, or instruction; and 4) personnel who routinely work in both controlled areas and restricted areas.

4.10.1. When the USAF Restricted Area Badge is used in place of the Controlled Area Badge, develop local procedures and publish them in a base instruction, security plan, or other official publication.

4.11. Training Personnel Who Work in Controlled Areas. Everyone who works in controlled areas receive initial and follow-on training from the unit controlled area monitor. Training and awareness is the most important part the controlled area program. An administratively flawless program is of no value if people working in and around controlled areas are not vigilant of suspicious activities occurring around them. Therefore, a strong controlled area training program advocates a questioning, inquiring attitude. Cover the following areas in your controlled area training program: 1) Properly protecting and wearing controlled area badges (if applicable); 2) what makes a controlled area “controlled” and why does the installation commander designate them as such? 3) challenge any person not wearing a badge or whose activity or presence in the area appears questionable; 4) methods for sounding the alarm and contacting the security police when you cannot verify another person’s identity or right to be in the area; and 5) reporting procedures when controlled area badges or other entry media are lost or stolen. Unit commanders must ensure such incidents are investigated.

4.11.1. Frequency of Training. Controlled area training is conducted prior to allowing unescorted entry into controlled areas. Conduct recurring training annually, or more frequently when directed by the installation commander or RPEC. Document and conduct training IAW local procedures.

Chapter 5

PROTECTING FUNDS AND OTHER HIGH VALUE RESOURCES

5.1. Overview. Most Air Force installations contain resources valued at over

100 million dollars. A respectable portion of this value is in the form of cash, precious metals, communication equipment, pharmaceuticals, electronics, resale merchandise, and other property which require adequate safeguards. With so much at stake it's easily understood why the protection of installation resources is everyone's responsibility. This chapter covers some of the most vulnerable property typically found on most military installations. It also reviews programming considerations which will help you determine your "resource protection climate" and allow you to assess current protection programs, develop new, or improve existing programs.

5.2. Who Must Comply. AFI 31-209 identifies the standards for the protection of funds and high value resources in the Air Force Resource Protection Program. The content of AFI 31-209 and this handbook generally do not apply to funds controlled by private organizations such as credit unions, the American Red Cross, commercial banks, airline ticket offices, etc. However, the CSP working on behalf of the installation commander, must encourage such activities to meet the protection standards outlined here and in AFI 31-209. The CSP should review the protection standards of non-government agencies to ensure adequate protection measures exist:

5.2.1. The protection requirements outlined in Exchange Operating Policy (EOP) 16-1, Loss Prevention, and any regional headquarters or local AAFES supplements guide AAFES facilities. Installation RPPMs should have access to and be familiar with that publication.

5.2.2. If a contractual relationship exists (for example, a concessionaire or commercial bank) make protection of funds part of the contract.

5.2.3 US Postal Service procedures regarding resource protection govern post offices, both conus and oversees. All post offices operated by Air Force Postal Squadrons will comply with AFI 31-209 and should review this handbook to ensure sound program management and administration.

One hundred percent compliance with Air Force standards by the above organizations and other non-government agencies is not required or intended. Rather, each agency must implement adequate resource protection measures that reasonably ensure the safety of non-government resources. The CSP must advise the installation commander and non-government agencies when their protective standards are lacking and negotiate with management to ensure implementation of adequate protection measures. The protection of Air Force resources and personnel is the primary consideration when dealing with commercial and non-government agencies. In extreme cases, and when all good faith negotiations have failed, installation commanders may have no recourse but to terminate commercial or non-government operations that jeopardize the security or safety of Air Force property or personnel.

5.3. MAJCOM Responsibilities. MAJCOMs should supplement resource protection directives as necessary to meet command needs. Each MAJCOM supporting a subordinate unit not located on an Air Force installation should specifically address resource protection requirements for that unit.

5.4. Responsibilities of the Installation Commander. The installation commander ensures adequate security for government funds and high cash value items. AFI 31-209 requires each installation commander prescribe in writing, the limits for storing funds during non-operating hours. The installation commander also (through the local RPEC) determines fund storage procedures for all facilities storing less than $100,000. This encompasses a broad range of installation facilities and indeed, perhaps all facilities with the possible exceptions of central depositories, finance offices, contract commercial banks, and the like. The installation commander has flexibility and authority under AFI 31-209 to meet the unique needs of the installation. Careful consideration and thorough staff work from the RPEC, CSP, and facility managers controlling funds and high value items is vital to the installation commander's decision making process.

5.5. CSP Responsibilities. The CSP ensures, on the installation commander's behalf, individual protection programs meet required Air Force or comparable protection standards. Always inform the installation commander when programs do not meet program requirements. Other CSP responsibilities include:

5.5.1. Provides staff supervision over protection programs of fund facilities.

5.5.2. Coordinating with contracting, procurement, supply, civil engineers, communications, and other support agencies to ensure they acquire, install, and maintain effective facilities and equipment for protecting government funds, including those belonging to tenant and geographically separated units (GSUs).

5.5.3. Test base anti-robbery procedures as prescribed in para 2.9 and AFI 31-209, Chapter 2.

5.5.4. Acting as the installation commander's representative during negotiations with non-government agencies in areas dealing with the protection of non-government funds and other valuables

5.5.5. Developing local procedures which cover authentication and duress procedures, access and opening/closing authority, verification procedures, fund container records, and other administrative procedures to ensure the security and safety of funds and high value property

5.5.6. Implementing adequate fund escort procedures as cited in AFI 31-209.

5.6. Responsibilities of the Funds or High Value Property Custodian. The custodian:
5.6.1. Ensures protection of funds or other property entrusted for care as prescribed in AFI 31-209, this handbook, and other resource protection publications.
5.6.2. Establishes written procedures for handling and safeguarding valuable property and ensures all employees are aware of those procedures.
5.6.3. Obtains written approval for funds and/or high value property handling and storage.

5.7. Funds Escort Procedures. The operation of fund or other high value property facilities will vary depending on local procedures and threat assessments. Consequently, procedures for moving those assets also vary. When moving funds or other high value items comply with the escort procedures contained in AFI 31-209, chapter eight, and AFH 31-218, Vol I, Law Enforcement Mission and Procedures, or more stringent standards as determined by the installation commander or RPEC. When possible, use commercial or contract escort services when moving funds off-base. When this is not possible, the CSP should ensure local police authorities understand the responsibilities and limits of security police authority off-base.
5.7.1. Special Procedures. The use of armed security police escorts off-base is governed by host nation agreements and local policies developed by the CSP, reviewed by the staff judge advocate, and approved by the installation commander. Overseas installations will develop alternative procedures where the arming of security police escorts is prohibited, or in the judgment of the installation commander, is not necessary or prudent. In such cases the installation commander may waive escort requirements contained in AFI 31-209.
Review local conditions and implement alternative procedures that ensure the best possible protection for off-base funds escorts.

5.8. Protecting Other High Cash Value Resources. Easy targets for theft include precious metal such as gold, silver, platinum, and other precious metal bearing scrap, as well as some recyclable materials. This is often because we don't recognize the item as having high value, and therefore fail to afford proper protection. Such items are listed in AFM 67-1, USAF Supply Manual, and are assigned a controlled item code "R" to identify them as having value beyond their intended purpose or configuration. These codes are fluid and change as a result of many factors. For example, you might not give roadway guard rails stacked in an open CE compound a second thought. But when the price for scrap aluminum climbed well above a dollar a pound in the late 1980's, thousands of guardrails began "disappearing" from our nation's highways. An item we gave little thought had suddenly become a lucrative target for late night thieves who made thousands of dollars removing, and selling as scrap, aluminum highway guardrails. This illustration proves only to remind resource managers that "value" is relative, and we must remain flexible and adaptable in our approach to resource protection.
5.8.1. Protect resources according to their current dollar value as prescribed in AFI 31-209 and this handbook. However, as with our example above, this is not always possible, particularly when items are:
5.8.1.1. Large and bulky
5.8.1.2. Integral parts of machinery, equipment, or items of supply
5.8.1.3. Intended for public display
5.8.1.4. Low in unit value and precious metal content
5.8.1.5. Protected under other programs
Note: Determining an item's replacement cost is one way of assessing its dollar value and potential for theft or misappropriation.
5.8.2. In situations where standard funds protection measures are not feasible or are impractical, the responsible commander for that property develops alternative protection recommendations which are staffed through the RPPM, CSP, and installation commander or RPEC. Document these procedures in your local supplement to AFI 31-209.
5.8.2.1. The security of computers and computer components is one resource that often requires special procedures. In large offices it's often impractical to secure each individual computer or computer component. Consequently some federal agencies have reported the theft of high value computer chips from office computers. In less than one hour, a trained thief can remove tens of thousands on dollars in computer chips that can be carried out in a container no larger (or more conspicuous) than a pack of cigarettes. A hollow core door with light duty lock was, in many cases, the only theft deterrent - woefully inadequate considering the known risk and high dollar value of computer chips and hardware. Therefore we must pay close attention to how computer hardware and software is protected. Medium or high security doors, barred windows, and IDS are possible solutions to increase security over areas containing high value computer and computer components.

5.9. Fund Container Requirements. Do not store funds, precious metals, jewels, or other items of high value in any container used to store classified material. High value item containers must meet specific Air Force and DoD certification

and construction standards. Unit resource protection focal points should check containers to ensure they meet standards outlined below. You may continue using containers not meeting standards if in the judgment of the unit commander, they provide satisfactory levels of protection. Consider the use of additional compensatory or security measures to counter security degrades caused by noncompliance containers. Remember, the container is only one part (and not the most important) of your overall resource protection program. Evaluate all protection measures and replace existing containers that fail to provide you a comfortable level of protection.

5.9.1. Insure containers used to store government funds meet GSA specifications. If the container does not meet GSA specifications, it must contain a Underwriter's Laboratory (UL) label (or foreign equivalent) certification as a burglar-resistant safe. You must also equip the container with a locking or relocking device. Those containers manufactured to a GSA specification have an external label reading "General Service Administration, Approved Security Container" along with the manufactures name. Additionally, the container should have an internal fixed label stating the federal specifications it was manufactured under and the protection it affords. Similar information is found in non-GSA approved containers having UL labels and information attached to them. Unit resource protection focal points should know this information. They should also know which of their safes and containers do and do not meet standards and any compensatory measures required. Refer to chapter 8, AFI 31-209 for types of safes required for various amounts of funds stored.

5.9.1.1. Use security containers manufactured to Federal Specifications AA-F-357, AA-F-358, AA-F363B, and AA-F-1518 for storing significant levels of cash or other high value material. Locks for approved security containers must meet Group 1 or 1R requirements specified in UL Standard Number 768. Obtain additional information concerning federal specifications and UL standards by consulting AFI 21-401, Engineering Data Storage, Distribution, and Control, and your RPPM.

5.9.2. Except for central depositories, secure fund and high value item containers weighing less that 500 pounds to the building to prevent their easy removal. This does not apply to containers located inside locked vaults. Coordinate with the base equipment manager, civil engineering, and the unit resource protection focal point to determine the best way to secure containers to the premise.

5.9.3. Place the container in the best position to enhance the detection of unauthorized access. A well lit container placed in front of an alarmed security window which allows easy observation from outside is one example of strategic container placement.

5.9.4. Carefully control the container combination and restrict it to the least number of people necessary. Follow the guidance in AFI 31-209 , chapter 8 regarding mandatory combination changes.

5.10. Fund Storage Rooms. According to AFI 31-209, facilities storing $100,000 or more in cash or cash value material must store those items in an approved alarmed vault or secure storage room. Facilities storing lesser amounts on a routine basis should also consider a vault or secure room storage. This determination is made by the installation commander based on judgment, RPEC recommendations, and the principles and concerns discussed throughout this handbook. Facilities requiring vault or secure room storage must comply with specific minimum engineering and construction standards. A funds storage room is a space specifically selected for containing a funds storage container. The room is intended to supplement funds container protection by providing protection in-depth. Choose a room small enough to keep the cost of protection as reasonable as possible while reducing theft vulnerability. Hardening of the room may vary based on several factors such as:

5.10.1. Value of the material stored

5.10.2. Type and level of protection afforded by the individual fund storage container(s)

5.10.3. Distance of the fund storage room from responding police or security forces

5.10.4. Presence of an IDS and its sophistication and reliability

5.11. Construction Standards. The criteria outlined below are minimum standards for fund storage rooms. Inspect rooms not previously certified for compliance. Upgrade existing fund storage rooms to ensure they meet minimum Air Force standards described below.

5.11.1. Doors:

5.11.1.1. Construct doors of 1 3/4 inch solid or laminated wood with 12-gauge steel plating on the outside face; or standard 1 3/4 inch hollow metal, industrial-type construction with minimum US 14- gauge skin plate thickness, internally reinforced vertically with continuous steel stiffeners spaced 6 inches maximum on center.

5.11.1.2. Rigidly anchor door bucks, frames, and keepers and provide antispread space filler reinforcement to prevent disengagement of the lock bolt by prying or jacking the door frame. Also, design and install the frames and locks for both interior and exterior doors to prevent removal of the frame which faces the built-in locking mechanism. Design frames to prevent spreading sufficiently to disengage the lock bolt from outside the protected room when the door is closed and locked.

5.11.1.3. Choose the construction requirements for door frames and thresholds as those for the doors. For example, where metal doors are used, use metal frames and thresholds. You may use a class 5 steel vault door (Federal Specification

AA-D-600B) with built-in, three position, changeable combination lock, instead of other doors or locks. Locks must conform to US Standard Number 768, Group 1R criteria.

5.11.1.4. Various types of hinges are commercially available. When choosing the proper type of hinge for secure area doors, apply the following criteria:

5.11.1.5. Choose a hinge strong enough to withstand the rigors of constant use and the high weight of the door.

5.11.1.6. Hinges will have fixed pins or equivalent

5.11.1.7. Peen, spot weld, or otherwise protect exposed hinge pins to prevent their removal. Do not expose hinge mounting screws to the outside. If exposed, modify them to prevent their removal.

5.11.2. Windows and Other Openings. Fill-in non-essential openings and seal with material comparable to that forming the adjacent walls, floor or ceiling. Keep openings limited to the essential minimum. Equip windows, ducts, vents, or similar openings large enough to permit entry (96-square inches or more with perimeter dimensions greater than six inches) with:

5.11.2.1. Three-eighths inch or larger hardened steel bars. Space vertical bars no more than 4-inches apart and weld horizontal bars to the vertical bars so that no opening exceeds 32 square inches.

5.11.2.2. High carbon manganese steel mesh (US Number 8-gauge) with 2-inch diamond grid

5.11.2.3. US Number-6 gauge steel mesh with 2 inch diamond grip when manganese steel mesh is not available.

Note: Securely embed bars and steel mesh in the structure of the building or weld to a steel frame that is securely attached to the wall with fasteners inaccessible from the interior of the facility.

5.11.3. Walls, Floors and Ceilings. Survey these areas to determine their resistance to forced entry. If necessary, reinforce them to provide penetration resistance at least equal to that of the doors and windows. Since reinforcement to these areas can involve expense, planers should survey base facilities and where feasible, use existing areas that meet storage room standards. Planners may also use additional IDS or other compensatory measures to protect resources when reinforced facilities are not available, or are structurally or financially impractical to modify.

5.11.4. Locks and Keys. Equip doors used for entry to funds and high value item storage areas with, as a minimum, locks and hasps meeting MIL-P-17802 standards, or a key-actuated deadbolt with at least a one inch throw. Develop strong key control measures similar to those discussed in chapter 6, para 6.9.

5.11.5. Lighting. Provide interior and exterior lighting for all facilities containing a controlled area funds storage vault or funds storage room per AFI 31-209. Lighting for other facilities is encouraged and is determined by the installation commander. Consider additional facility checks or other compensatory measures for facilities having inadequate lighting. The CSP should review all funds and high value storage facilities and present the RPEC with a prioritized list of facilities in need of basic or additional lighting. Basic lighting must allow persons observing the facility to recognize illegal acts such as breaking and entering during hours of reduced visibility. Place lighting at strategic locations to reduce areas where someone might hide. Place switches and wiring conduits to avoid bypassing or tampering by unauthorized personnel. Units may use motion activated lighting systems or similar devices that allows reduced lighting to save energy. Ensure these cost cutting measures do not prevent or degrade the purpose of lighting.

5.12. Use of IDS. The use of IDS is very effective in reducing theft of funds and other high value items. Provide facilities requiring protection under AFI 31-209, with at least two levels of alarm. IDS for facilities storing lesser amounts is determined by the installation commander or RPEC. Remember, the baseline requirements outlined in AFI 31-209 represents the ideal resource protection climate. Lesser amounts of funds stored in non-hardened facilities without IDS may prove very vulnerable to theft. Evaluate installation funds and high value storage facilities not requiring IDS under AFI 31-209, for the need for hardening and/or IDS. The CSP should conduct program reviews of those facilities and forward a prioritized recommendation to the installation commander or RPEC, who in turn determine which facilities may require hardening, the installation of IDS, or both.

5.13. Standards for Non-government Facilities. As a general rule, non Air Force, non-DoD facilities are not required to comply with Air Force or DoD funds protection standards. Their participation in the installation resource protection program (program reviews, RPEC participation, anti-robbery exercises, etc) is also voluntary. However, this does not mitigate the installation commander's responsibility to protect personnel and property on the installation, regardless of their military or civilian affiliation. Each installation commander determines if protection measures taken by non-military agencies is adequate. When necessary, installation commanders may have to balance potentially incompatible situations with persuasion, negotiation, and where warranted, financial assistance to ensure all base assets are properly protected. Report situations which you can not resolve up the chain of command. Where possible, notify the appropriate civilian agency headquarters counterpart involved in the disagreement, i.e., corporate president, regional office manager, chairman of the board, etc. Installation commanders may modify or terminate any operation that posses a hazard to the security or safety of their installation.

Consider such action only under extreme conditions and after good faith negotiations have failed. Coordinate such action through the Staff Judge Advocate and chain of command.

5.14. IDS Selection. Evaluate each funds storage facility/vault for both adequate protection and cost effectiveness. Hardness of the facility and the type and sophistication of IDS should vary depending on threat assessment and vulnerability. Consider the following criteria when installing IDS:
5.14.1. Select an IDS that provides complete protection for both the fund container and the area surrounding the container. Provide at lease two levels of alarm protection.

NOTE: Boundary detection alone is not an acceptable IDS for most funds storage rooms.
5.14.2. Magnetic door switches alone do not provide adequate perimeter detection for funds storage rooms. Install another IDS component to provide complete boundary detection.
5.14.3. A capacitance alarm that detects attempts to tamper with a funds container is considered an adequate level of detection. Applying point protection directly to a funds storage container is not required.
5.14.4. When more than one IDS is planned, assure system compatibility so that you can use a single centralized annunciator panel.

5.15. Duress Alarm Criteria. All fund storage facilities and vaults require duress alarms. Many other facilities may also require use of duress alarms as determined locally by the installation commander or RPEC. Base your duress requirements on dollar value of material stored and the local threat and risk analysis.

5.16. Testing IDS and Duress Alarms. Test IDS and duress alarms regularly to ensure they operate properly. Develop test procedures locally and ensure you consider manufacturer instructions when using non-standard systems.

5.17. IDS Failure. An individual (normally a facility custodian or owner/user person) must respond to all fund storage facilities or vaults when IDS or other protective measures become inoperable. Continuous surveillance is required until the system is restored, the funds or high value items are relocated to an equal or higher standard facility, or other protective measures are taken which ensures the security of the material. While providing surveillance, the individual must have a capability (radio, telephone, or duress alarm) to notify an armed response force should he/she detect unauthorized activity. Arming of the individual is determined locally by the installation commander or RPEC. The installation commander also determines response requirements for other facilities. The CSP should serve as principle advisor to the decision making authority.

Chapter 6

PROTECTION OF ARMS, AMMUNITION AND EXPLOSIVES (AA&E)

6.1. General Information. Military AA&E are lucrative targets for theft, attract a variety of threats, and are among our most vulnerable resources. During wartime, opposing forces may target them for their destructive power and ability to influence campaign outcomes on either side. During peacetime its the terrorist and criminal element that poses a constant threat. One of your greatest challenges is to protect these assets from the “enemy.” The guidance that follows will help you reach that goal. It is designed for use with AFI 31-209, DoD 5100.76-M, and their associated references. Together, they implement the resource protection criteria for the Air Force, Air National Guard (ANG). and Air Force Reserve (AFRES). Chapter 2 of this publication identifies generic procedures for exceptions to these criteria.

6.2. AA&E Protection. Everyone must ensure AA&E resources receive protection at all times. The installation commander (via RPEC recommendation) determines and approves both the number and location of all firearm storage facilities. Commanders designate all AA&E storage facilities as controlled areas, and identify in writing who is responsible for them and who is authorized unescorted access into them. Closely scrutinize each storage facility and reduce and consolidate facilities where possible. Commanders must also ensure adequate local written guidance covers the subjects and procedures contained in resource protection directives.

6.3. AA&E Categories. A risk category is assigned to all AA&E items in the DoD inventory. The DoD and Air Force have four AA&E risk categories. They are: Very High Risk (category I); High Risk (category II); Medium Risk (category III); Low Risk (category IV). Not all categories of resources have items in each category. For example, there are various missile and

rockets found in the first three categories but none in the fourth. Firearms on the other hand, are found only in the 2nd, 3rd, and 4th category, with none in the 1st category. This may seem confusing but the DoD and Air Force have determined that, because of their destructive power, there are no Low Risk (category IV) missiles and rockets. Conversely, and because of their limited destructive power, there are no Very High Risk (category I) firearms. As for ammunition and explosives, they are found in all four categories. DoD 5100.76-M contains additional guideline for codes pertaining to most AA&E items. To determine a specific risk category of a particular weapon or weapon component, consult the Stock Number User Directory available at your supply squadron. Likewise, protection standards are based on the type and vulnerability of a particular AA&E item. The following is a description of the various DoD categories for AA&E items:

6.3.1. DoD Category I Very High Risk (Missiles/Rockets/Ammunition and Explosives). Commanders afford the highest degree of protection for this category, as they pose a grave threat to any installation, its mission, and the safety of people if they become lost or stolen. Their compact size, ease of operation, and destructive power make them lucrative targets for both the criminal element and opposing military forces. The following includes examples of Very High Risk items:

6.3.1.1. Manportable missiles and rockets when in a ready to fire configuration. Included in this group are Redeye, Stinger, Dragon, Javelin, light antitank
weapon (LAW) and similar missile and rocket systems. Note: When the launcher tube and/or gripstock is stored or transported with the explosive rounds, then “ready to fire configuration” protection standards apply. When complete systems are installed in aircraft they remain Very High Risk items.

6.3.2. All explosive packs, detonators, and rounds for category 1 systems.

6.3.3. DoD Category II High Risk (Missiles/Rockets/Firearms/Ammunition and Explosives). Many items in this category, though sometimes more destructive then those in category 1, require special knowledge, launch platforms, or data systems to operate. These weapons generally have lesser appeal to opposing forces than category I weapons. However, they still require a high degree of security. The following includes examples of category II weapons.

6.3.3.1. Crew-served missiles and rockets or those that require platform-mounted launchers and complex hardware and software equipment to function. This group includes the tube-launched optically tracked weapon (TOW) and Hydra-70.

6.3.3.2. Light automatic weapons up to and including .50 caliber. Also included is the 40mm grenade launcher, MK1 machine gun, M-16 and M-16A1 rifles and the like.

6.3.3.3. All weapon components such as silencers, mufflers, and other noise suppression devices

6.3.3.4. Hand or rifle grenades, high explosives and white phosphorous

6.3.3.5. Anti-tank or anti-personnel mines having an unpacked weight less than
50 pounds each.

6.3.3.6. Explosives used in demolition operations, C-4, military dynamite, and TNT having an unpacked weight less than 100 pounds.

6.3.3.7. Warheads for sensitive missiles and rockets weighing less than 50 pounds each

6.3.3.8. Binary intermediates “DF” and “QL” when stored separately from each other and from the binary chemical munition bodies that they are intended to employ from.

6.3.4. DoD Category III Medium Risk (Missiles/Rockets/Firearms/Ammunition and Explosives). Weapons in this category generally include an extension of those found in category II except their construction, weight, requirements to operate, and other factors make them less desirable to opposing forces. Weapons of this category require strong security and safeguard measures. The following includes examples of category III weapons:

6.3.4.1. Missiles and rockets that require platform-mounted launchers and complex hardware and software equipment to operate. Included in this group is the Hellfire missile.

6.3.4.2. Launch tube and gripstocks for Stinger missiles. Launch tube, sight assembly and gripstock for Hamlet and Redeye missile.

6.3.4.3. Grenade launchers (except 40mm) and flame throwers

6.3.4.4. Most ammunition 50 caliber and larger containing explosive filled projectiles, each weighing 100 pounds or less.

6.3.4.5. Incendiary grenades and fuses for high explosive grenades

6.3.4.6. Blasting caps

6.3.4.7. Supplementary charges

6.3.4.8. Bulk explosives and detonating cord

6.3.4.9. Warheads for sensitive missiles and rockets weighing more than 50 pounds but less than 100 pounds each.

6.3.5. DoD Category IV Low Risk (Firearms/Ammunition and Explosives). This is the lowest DoD risk category requiring protection. Most items in this category do not pose a great threat to military resources if lost or stolen, but because of their toxicity and the inherent danger they pose to others, require safeguarding at all times. Examples of some category IV items:

6.3.5.1. Shoulder fired weapons, other than grenade launchers, not fully automatic

6.3.5.2. Handguns (not fully automatic)

6.3.5.3. Recoilless rifles up to and including 90mm

6.3.5.4. Fuses, grenades (illumination, smoke, tear gas, marker, etc.)
6.3.5.5. Ammunition with nonexplosive projectiles having unpacked weights of 100 pounds or less.
6.3.5.6. Fuses, except for those listed as medium risk
6.3.5.7. Incendiary destroyers
6.3.5.8. Riot control agents
6.3.5.9. Ammunition for category II, III, and IV weapons (not otherwise categorized)
6.3.5.10. Explosive compound for sensitive missiles and rockets (except warheads)

6.4. AA&E Storage Facility Defined. A storage facility is a structure used for housing, on a routine basis, any number of category I or II AA&E items or more than 30 category III items. Unless specifically addressed, the criteria in this publication (which reflects those found in numerous DoD and Air Force publications) applies to AA&E storage facilities. A facility storing no category I or II items, or fewer than 30 category III items is not an AA&E facility unless so designated by the MAJCOM or installation commander. The MAJCOM or installation commander determines protection standards for Non-AA&E facilities. AA&E facilities must meet rigorous construction and security standards contained in AFI 31-209, DoD 5100.76-M, and other DoD and Air Force publications cited later in this chapter.
6.4.1. Entering AA&E Facilities. At least one person should be armed before entering an unmanned AA&E facility. If this is not possible, the person should arm themselves as soon as possible after entering. At least one AA&E facility attendant remains armed at all times while on duty. Develop local procedures to ensure verification and authentication with the appropriate police agency before entering or securing any AA&E facility.

6.5. IDS Requirements. Standards and procedures for protecting AA&E items vary according to their risk category. The protection measures outlined below are minimum standards set by DoD. Installation commanders must consider their installation's threat profile, vulnerability, mission, and available resources when determining local requirements. The mission and profile of each installation may dictate application of more stringent standards.
6.5.1. Protection Requirements for DoD Category I and II (Very High and High Risk). Unless continually manned by owner/user personnel, or when unoccupied, under continuous surveillance by an armed guard, protect category I and II AA&E facilities with at least two levels of IDS, one a form of penetration detection, the other, either motion or point detection. Refer to paragraph 3.10.9. for definitions and additional IDS information. A duress alarm is also required and must enunciate at a 24 hour manned facility capable of notifying security forces and sounding the alarm. Do not locate this manned facility in the same building or structure housing the weapons. Exception: Same facility duress alarm is allowed if the alarm terminates at the law enforcement desk, central security control, or other area manned by armed police or security6.5.2.
Protection Requirements for DoD Category III and IV (Medium and Low Risk). The installation commander determines manning requirements for facilities housing category III and IV AA&E resources. IDS is not required for on-base facilities housing only category III or IV resources. However, installation commanders should carefully consider the installation of IDS (or other protection enhancing measure) if an on-base facility routinely stores large numbers of category III and IV AA&E. IDS is required for all off base facilities storing any number of category III or IV items. A duress alarm is also required (refer to para 6.5.1.) for all category III and IV facilities unless located inside a priority A restricted area.

6.6. Facility Checks. Check the exterior of unmanned AA&E storage facilities containing category I and II items at least once every 24 hours. The installation commander may require more stringent requirements if necessary. Give greater consideration to those isolated facilities or those hidden from view, or located outside a reasonable security police response time. Also consider lighting and structural deficiencies, ease of access, and other factors. Locally determine the need to physically enter facilities and visually inspect the items. Local policy also determines who performs the checks, when to conduct them, and frequency of checks when more than one check per day is required. For storage areas where IDS is optional but is not used, conduct checks more frequently then once each day.
6.6.1. Determine facility check frequency for category III and IV facilities locally. You can authorize any competent individual to conduct checks, however, the CSP will determine if and when to arm those conducting after duty hour checks. Train personnel to conduct checks and ensure they are under the supervision of a police or security activity. Note: Radio contact, telephone authentication/verification, or other control features that allow police or the security activity to monitor progress of the check meets DoD criteria requiring checks by a "supervised guard patrol."

6.7. Emergency Power and Lighting Requirements. Installation commanders determine which AA&E storage facilities require emergency power and lighting. During power outages, owner/user or security personnel will respond as soon as possible to man facilities containing category I and II resources. Locally determine procedures for category III and IV facilities. Personnel responding must be armed or capable of sounding the alarm to a 24 hour manned police or security facility. Man category I and II facilities until power is restored, the AA&E items are relocated to a functioning facility, or other

measures are taken which ensures security and integrity of the material. Determine protection for emergency power sources locally.

6.7.1 Consider the following questions when deciding when and if to use emergency power for AA&E facilities at your installation:

6.7.1.1. How many and what class of AA&E items are stored?

6.7.1.2. What is the hardness and security of the storage structure, i.e., portable magazines versus hardened, high security concrete bunkers?

6.7.1.3. What is the response time of owner/user personnel once commercial power fails?

6.7.1.4. Location of the storage area and their degree of isolation

6.7.1.5. Number of security patrols and can they randomly check storage facilities until owner/user personnel arrive

6.7.1.6. Local threat climate

6.8. Security Lighting. Provide exterior lighting for all category I and II AA&E storage buildings, buildings in which these items are located, and all controlled entry doors to arms rooms. Exterior lighting should allow an individual to see unauthorized activity, such as forced entry, or the unauthorized removal of arms during hours of reduced visibility. Install switches for exterior lights so they are not accessible to unauthorized persons. Locally determine procedures for category III and IV facilities.

6.9. Key and Lock Control. Maintain keys to all AA&E firearm storage buildings, rooms, racks, containers, and keys to alarm systems supporting those areas separately from other keys. Keep the number of keys to the absolute minimum essential and provide access only to those whose official duties require it. Units may use a master key system for storage racks and containers. Do not use a master key system for facility entry doors or individual storage rooms. Keep keys secure at all times. Commanders responsible for weapons storage facilities and/or weapons issue must maintain an access letter designating those authorized to have keys to weapons areas. Keep this letter, as well as other documents outlining weapons access procedures and operations from public view. Additionally, the procedures below apply to key and lock control:

6.9.1. Secure keys providing access to category I or II weapons facilities in a Class 5 GSA approved security container or equivalent.

6.9.2. Secure keys providing access to category III and IV weapon facilities in containers of at least 20 gauge steel, or material of equivalent strength and equipped with a GSA approved built in changeable combination lock, or a GSA approved key operated medium or higher security padlock.

6.9.3. Duty officers, security supervisors or others who don't have unescorted access, must sign for sealed containers of keys when responsible for safeguarding or having keys immediately available.

6.9.4. Do not remove keys to arms storage from the installation except to provide for storage elsewhere.

6.9.5. Installation Commanders or their designee appoint in writing, a lock and key custodians.

6.9.6. Maintain a key control register to ensure continuous administrative accountability for keys. Accountability records must have the signature of the individuals receiving and issuing keys, the key number or other identifying data, and the date and time of key issue and return.

6.9.7. Maintain key issue logs for a minimum of 90 days and then dispose of them in accordance with local procedures and AFM 37-139.

6.9.8. Key Inventories. Conduct a key inventory of all firearm storage facilities at least semiannually. Locally establish more frequent inventories, if required.

6.9.9. Maintain inventory records for at least one year. Locally determine maintenance beyond that period.

6.10. Inventories. Conduct AA&E inventories according to AFM 23-110, Vol 2, chapter 20, AFI 31-209 chapter 5, and DoD 5100.76-M, Chapter 6. At unit level the more stringent standards in AFI 31-209 will prevail over lesser standards contained in the DoD publication. AFI 31-209 standards do not apply to depots, freight yards, shipyards, and some large base level storage facilities. Base level facilities are defined as infrequently entered storage and magazine areas containing AA&E items for contingency, mobility, emergency, or other reasons that require they not be issued, used, or handled on a frequent basis. Example: A properly secured and sealed supply storage vault not entered on a regular basis would not require daily inspections, but instead, could be inspected semi-annually according to DoD 5100.76M standards. Installation commanders are in the best position to determine which, if any, of there facilities qualify as a base level storage facility and may authorize the use of the lesser DoD standard. AFI 31-209 standards are intended for "working" arms room facilities and have proven highly effective in reducing, to very low levels, the number of weapons and munitions lost or stolen from those facilities.

6.11. Protecting Weapons Under Field Conditions. Put category I and II weapons used under field conditions under constant surveillance when normal protection hardware such as vaults, IDS, etc., are not available. The installation

commander, or deployment force commander, determines any additional protection standards. Carefully consider the number and class of weapons in use, location where used, current threat, availability of armed response forces, and other factors when determining adequate protective measures. If possible, the users or accompanying personnel should have radio or telephone communication with a 24 hour work center capable of sounding the alarm and notifying an armed response force. If using Category I or II weapons, the responsible agency should strongly consider using an armed protective escort.

6.12. Exceptions to Protection Standards. When approved by the installation commander, on base units may store small quantities of class II weapons in a class five GSA approved or equivalent container with a combination lock. Do not approve exceptions unless all other storage vault requirements, applicable to class II storage, i.e., IDS, key control, manning requirements, etc., exist. Consider additional checks or compensatory measures depending on the location of the facility considered for waiver, and the overall resource protection "climate" of the installation. Do not use this exception to avoid the requirement for certified weapons storage vaults and containers meeting DoD specifications.

Note: "Small quantities" is defined as 10 or fewer class II weapons.

6.13. Transporting Weapons. Weapons are very vulnerable during transportation. Air and surface freight, as well as commercial airline transportation cause particular concern. DoD 5100.76-M and DoD 4500.32-R, Military Standard Transportation and Movement Procedures (MILSTAMP), March 1987, governs in-depth, the transportation of AA&E by military and commercial means. They also cover physical security standards at military, commercial, and contractor facilities, escort requirements, postal shipments and other transportation methods. The installation's transportation squadron commander, chief, traffic management section, or equivalent, must remain knowledgeable of the shipping and safeguarding requirements contained in those publications. Additionally, the following applies to the shipment of firearms.

6.13.1. Transporting Weapons in Motor Vehicles. Unless prohibited by MAJCOM or local procedure, you may transport all categories of weapons on or off base in government owned vehicles (GOV). The transportation of category III and IV, as well as small quantities of category II weapons (10 or fewer) in privately owned vehicles (POV) is authorized unless specifically prohibited. When using POVs to transport weapons off base, ensure full compliance with local requirements and ordinances. Coordinate off base transport of class I and II weapons with local authorities. Do not transport Category I weapons in POVs except under emergency conditions. When transporting category I or II weapons, arm escorts IAW AFI 31-209. The arming of escorts for category III and IV movements is determined locally. When making that determination, consider the number and category of weapons being escorted, local threat, distance, terrain, and other factors.

6.13.2. Shipping Military Arms on Non-military Aircraft. Military aircraft, or military contract commercial air is the preferred method for shipping firearms. However, when time and circumstances do not allow the use of military aircraft, the use of commercial aircraft for weapons shipment is authorized. When shipping weapons by commercial air-carriers, you must adhere to shipping instructions contained provided by the local Transportation Management Office (TMO), and the local air carrier. Unless prohibited by a local air carrier or other publication, you may ship category III, IV, and small numbers of category II weapons on commercial airlines. Consider carefully the destination, number of stops and transfers, potential for theft enroute or upon arrival at final destination, number of pervious thefts, if any, and the safeguards and procedures established by the carrier. TMO personnel should consult the US Government Foreign Clearance Guide, RPPM, local Office of Special Investigations (OSI), and other sources and information to evaluate air carrier and terminal security at departure, destination and stops in between. Personnel shipping military small arms must ensure they are shipped in locked or banded crates, lockable hard-shell gun cases, or other suitable containers affording reasonable security. Soft side gun cases, mobility bags, and the like are not suitable shipping containers. You must ship weapons separately from all personal gear. Ensure orders or other unit identifying information is contained inside the shipping container.

6.14. Additional Requirements for DoD Category I and II Ammunition/Explosives. When possible, consolidate and maintain ammunition and explosives in an on-base nonnuclear munitions storage area. Refer to AFI 91-409, Explosive Safety Standards, for additional storage guidance. The installation commander designates all ammunition/explosive storage areas as controlled areas. Commanders using ammunition/explosive storage facilities designate in writing those authorized unescorted access to ammunition/explosives. To the greatest degree possible, develop local procedures which prevent unauthorized access when multiple users have access to consolidated storage areas, i.e., an individual authorized access to category III items is allowed unescorted access to category I items. Where possible, segregate explosive storage facilities (bays, bunkers, rooms, etc.) by type and class to eliminate unnecessary access to higher class items. In addition to the following, the standards contained in para 4.5 through 4.8 apply to category I and II ammunition and explosives.

6.14.1. Field Conditions. Constant surveillance by an armed individual is required when stored in facilities without IDS. This requirement applies to storage and does not necessarily apply to small quantities used under field conditions for training, maneuvers, or when temporarily held for immediate application. In this case put emphasis on immediate use and application

versus storage. Regardless, responsible commanders must ensure adequate security and safeguard procedures are implemented when category I and II items are removed from their normal storage facilities.

6.14.2. Fencing. Category I and II storage areas require fencing. Refer to DoD 5100.76-M for construction criteria.

6.14.3. Security Lighting. Requirements under paragraph 6.8 apply for category I and II Munitions and Explosives storage areas. The installation commander or RPEC determines security lighting requirements for category III and IV areas.

6.14.4. Emergency Power and Lighting Requirements. Emergency lighting and standby power is not required. However, commanders should consider installing such systems when location, threat, and vulnerability warrant. Also consider the type and amount of substance stored. During power outages, the manning requirements in paragraph 6.7 apply to category I and II munitions and explosives storage areas. The installation commander or RPEC locally determines manning requirements for category III and IV areas.

6.14.5. Vehicle and Pedestrian Entry Control Requirements. Except as otherwise directed, each installation commander or their designee determines entry control procedures for munitions storage areas. Secure entry points and maintain strict key control for vehicles and personnel entering munition storage areas. A system of random inspections of vehicles and personnel entering and leaving the facility or area is mandatory according to DoD 5100.76 -M, chapter 5. Maintain entry records to munitions storage facilities until the next weapon/munition inventory is completed. Prohibit privately owned vehicles in the magazine or storage area.

6.14.6. Key and Lock Control. Secure magazines with a high security locking system. Use a class 5 or 8 steel vault door with a built-in combination lock, or a high security padlock and hasp on doors to structures housing classified material. Refer to paragraph 6.9 for additional key control and custodial requirements.

6.15. Additional Requirements for DoD Category III and IV Ammunition/Explosives.

6.15.1. Structure Needs. Facility (storage) construction requirements for category III and IV are contained in DoD 5100.76M and DoD 6055.9-STD. Also refer to MIL-HDBK 1013/1, Design Guidelines for Physical Security of Fixed Land-Based Facilities, for materials and construction techniques that will afford a minimum of a ten minute forced entry delay. When mission requirements, safety, and ease of operations allow, collocate category III and IV storage in or adjacent to existing category I and II facilities. Centralized locations reduce operating costs and reduce the number of potential targets for theft.

6.15.2. Field Conditions: The installation commander or deployment force commander determines security requirements for category III and IV items used during exercises, deployments, and field conditions. Follow the considerations discussed in chapter 2 when making those determinations.

6.15.3. Fencing. The fencing of category III and IV storage facilities is optional.

6.15.4. Intrusion Detection Systems. IDS is required in all off base category III and IV munition storage facilities. IDS is optional for on-base class III or IV storage facilities and is determined locally by the installation commander. Consider carefully your location, mission, threat assessment, available manpower, criticality of the items requiring protection, and other factors unique to your situation.

6.15.5. Patrols. Owner/user or security forces must check Category III and IV Storage facilities with operational IDS at a minimum once every 24 hours. Locally determine the need for more stringent requirements. Munitions not protected by IDS or monitored surveillance cameras, but otherwise meeting all other storage and construction criteria require more frequent checks as determined locally by each installation commander. Facilities not meeting at least one of the above standards require constant owner/user or security supervision. Ensure personnel conducting checks can sound the alarm. Develop local procedures to ensure the security of category III and IV resources removed from, or contained in, facilities not meeting DoD and Air Force standards.

6.15.6. Installed or In-Use Munitions. The Air Force considers any munitions installed in aircraft, parachutes, life support, and so on as “in use”. Secure and protect these munitions as part of the whole weapons system IAW AFI 31-209. In unclear areas, or when there are questions, contact your base RPPM or CSP.

RICHARD A. COLEMAN, Brigadier General, USAF
Chief of Security Police

GLOSSARY OF REFERENCES, ABBREVIATIONS, AND ACRONYMS

References:

D/CID 1/21, *Director of Central Intelligence Directive*
DoD S-5105.21-M-1, *Sensitive Compartmented Information Administrative Security Manual*
DoD 4500.32-R, *Military Standard Transportation and Movement Procedures (MILSTAMP)* , March 1987
DoD 5100.76-M, *Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives*
DoD 6055.9-STD, *DoD Ammunition and Explosive Safety Standards*
DoDR 5200.1R, *Information Security Program Regulation*
AFI 21-401, *Engineering Data Storage, Distribution, and Control*
AFI 31-101, *The Air Force Physical Security Program*
AFI 31-209, *The Air Force Resource Protection Program*
AFI 31-401, *Managing the Information Security program*
AFI 91-409, *Explosive Safety Standards*
AFH 31-104, *Air Force Sensor Handbook*
AFH 31-218, Vol I, *Law Enforcement Mission and Procedures*
AFH 31-1084, *Standard Facilities Requirements*
Mil-Hdbk-1013/1A, *Military Handbook, Design Guidelines for Physical Security of Fixed Land-Based Facilities*
AFM 14-304, *The Security Use, and Dissemination of Sensitive Compartmented Information (SCI)*
AFM 67-1, *USAF Supply Manual*
AFM 23-110, *USAF Supply Manual, Volume II*
AFM 37-139, *Records Disposition Schedule*
USAF INTEL 201-1, *The Security, Use, and Dissemination of Sensitive Compartmented Information*
EOP 16-1, *Exchange Operating Procedure, Loss and Prevention*

Abbreviations and Acronyms

AA&E−Arms, Ammunition, and Explosives
AAFES−Army and Air Force Exchange Service
AECS−Advanced Entry Control Systems
AFM−Air Force Manual
AFRES−Air Force Reserve
ANG−Air National Guard
CPTED−Crime Prevention Through Environmental Design
CSP−Chief or Security Police
DECA−Defense Commissary Agency
DCID−Director of Central Intelligence Directive
DoD−Department of Defense
DoDI−Department of Defense Instruction
DoDR−Department of Defense Regulation
EOP−Exchange Operating Procedure
GOV−Government Owned Vehicle
GSU−Geographically Separated Unit
IAW−In Accordance With
ICIDS−Integrated Commercial Intrusion Detection Systems
IDS−Intrusion Detection Systems
IRPP−Installation Resource Protection Plan
ISP−Installation Security Plan
J-SIIDS−Joint Service Interior Intrusion Detection System
MIL-HDBK−Military Handbook
MILSTAMP Procedures−Military Standard Transportation and Movement
NCOIC−Noncommissioned Officer in Charge
NMSA−Non-nuclear Munitions Storage Area
OIC−Officer in Charge
OSI−Office of Special Investigations
POV−Privately owned vehicle
RPEC−Resource Protection Executive Council

RPPM−Resource Protection Program Manager
SCIF−Sensitive Compartmented Information Facility
SJA−Staff Judge Advocate
TMO